A: Ref KB
Occ SOU
43

Statens offentliga utredningar
1996:40
Justitiedepartementet

Elektronisk dokumenthantering

Betänkande av IT-utredningen
Stockholm 1996

SOU och Ds kan köpas från Fritzes kundtjänst. För remissutsändningar av SOU och Ds svarar Fritzes, Offentliga Publikationer, på uppdrag av Regeringskansliets förvaltningskontor.

Beställningsadress: Fritzes kundtjänst
106 47 Stockholm
Fax: 08-20 50 21
Telefon: 08-690 91 90

Svara på remiss. Hur och Varför. Statsrådsberedningen, 1993.
- En liten broschyr som underlättar arbetet för den som skall svara på remiss.

Broschyren kan beställas hos:
Regeringskansliets förvaltningskontor
Arkiv- och informationsenheten
103 33 Stockholm
Fax: 08-790 09 86
Telefon: 08-405 24 81

Graphic Systems AB, Göteborg 1996

ISBN 91-38-20210-7
ISSN 0375-250X

Till statsrådet och chefen för Justitiedepartementet

Regeringen beslutade den 19 maj 1994 att tillkalla en särskild utredare med uppdrag att utarbeta de förslag till rättslig reglering som kan behövas i samband med inrättandet av s.k. elektroniska anslagstavlor och för användningen av elektroniska dokument inom både förvaltningen och näringslivet.

Till särskild utredare förordnades den 17 juni 1994 generaldirektören Hans Jacobson.

Att som experter biträda utredningen förordnades fr.o.m. den 20 april 1995 avdelningsdirektören Göran Axelsson, jur. kand. Simon Corell, universitetslektorn Jan Evers, teknologie dr. Viiveke Fåk, datarådet Ingela Halvorsen, numera kanslirådet Martin Holmgren, kanslirådet Björn Rosén, distriktsåklagaren Christer Ström, förbundsjuristen Anne Wigart och förste arkivarien Britt-Marie Östholm, fr.o.m. den 17 maj 1995 hovrättsassessor Karin Göransson och fr.o.m. den 22 maj 1995 kanslirådet Catharina Staaf.

Till sekreterare förordnades fr.o.m den 1 september 1994 hovrättsassessor Per Furberg.

Utredningen, som antagit namnet IT-utredningen, får härmed överlämna betänkandet Elektronisk dokumenthantering (SOU 1996:40). Särskilda yttranden har avgetts av experterna Göran Axelsson och Ingela Halvorsen.

Utredningsuppdraget är härmed slutfört.

Stockholm i mars 1996

Hans Jacobson

/Per Furberg

Innehåll

Förkortningar 11

Sammanfattning 13

Summary 15

Författningsförslag 25
1 Förslag till lag om elektroniska förmedlingstjänster 25
2 Förslag till lag om ändring i brottsbalken 27
3 Förslag till lag om ändring i rättegångsbalken 28
4 Förslag till lag om ändring i lagen (1915:218) om avtal och andra rättshandlingar på förmögenhetsrättens område 30
5 Förslag till lag om ändring i delgivningslagen (1970:428) 31
6 Förslag till lag om ändring i förvaltningsprocesslagen (1971:291) 35
7 Förslag till lag om ändring i datalagen (1973:289) 37
8 Förslag till lag om ändring i sekretesslagen (1980:100) . 38
9 Förslag till lag om ändring i förvaltningslagen (1986:223) 39

1 *Utredningsuppdraget och dess genomförande* 43

Avdelning I
Elektronisk dokumenthantering i förvaltningen

2 *Utgångspunkter* 47
2.1 Inledning 47
2.2 Lagstiftning rörande elektroniska dokument, m.m. 48
2.3 Utvecklingen i Sverige och internationellt 49
2.3.1 Den offentliga verksamheten i Sverige 49
2.3.2 Internationellt arbete 50
2.4 Uppdraget 51
2.5 Förslagets inriktning 52
2.6 Vissa akuta behov av IT-anpassningar 54
2.7 Lagstiftningstekniken, m.m. 55
2.8 Vissa begrepp 56

3 *Inkommande handlingar* 59
3.1 Gällande rätt — traditionella handlingar 59
3.2 Gällande rätt och tidigare utredningsförslag — elektroniska handlingar 60
3.3 Överväganden 62
3.3.1 Överbringande av disketter och överföring via nät 63
3.3.2 Brevlådans fysiska placering är inte avgörande . 64
3.3.3 Kommit en behörig tjänsteman till handa 65
3.3.4 Särskilt om telefax 66
3.3.5 En hjälpregel för oklara fall? 67
3.3.6 Särskilt om telegram, m.m. 69
3.4 Tekniska och administrativa hinder mot att läsa inkomna data 70
3.5 Bekräftelse av handlingar som saknar underskrift i original 72

4 *Elektronisk delgivning* 75
4.1 Utgångspunkter 75
4.2 Nuvarande reglering 76
4.2.1 Delgivning eller mer formlös kommunikation . . 76
4.2.2 Formerna för delgivning 76
4.2.3 När skall delgivning anses ha skett? 77
4.2.4 Begreppet handling 78
4.3 Överväganden 79
4.3.1 Delgivning och kvittering med signerade handlingar 79
4.3.2 Delgivning utan digitala signaturer eller stämplar 80
4.3.3 E-post som ersättning för vanlig postdelgivning 81
4.3.4 Förenklad elektronisk delgivning 85
4.3.5 En definition av elektronisk handling, m.m. . . . 88

5 *Elektroniska handlingar som ersättning för undertecknade handlingar m.m.* 91
5.1 Vilka myndigheter berörs? 91
5.2 Vilka regelverk berörs? 92
5.3 Vissa begrepp i FL 93
5.4 Området utanför FL 95
5.5 Mitt förslag 97
5.6 Normgivningskompetensen och den föreslagna bestämmelsen 98

6 *Övriga frågor* 101
6.1 Offentlighetsinsynen 101
6.2 Sekretess för koder m.m. 104
6.3 Skyddet för persondata 105

6.4 Arkivfrågor 112
6.5 Konsekvenser av mina förslag 114

Avdelning II
Elektronisk dokumenthantering inom näringslivet

7 *Bakgrund* 117

8 *Avtalsrättsliga frågor* 119
8.1 Utgångspunkter 119
8.2 Behovet av översyn 121
8.3 Att sända och motta förklaringar 123
8.3.1 Rättsverkningar genom avsändande 123
8.3.2 Rättsverkningar genom mottagande 125
8.3.3 Frister vid skriftlig respektive muntlig kommunikation 128
8.3.4 Tillämpningen av vissa regler som kräver mänskliga förhållningssätt 129
8.3.5 Särskilt om befordringsfel 132

9 *Övriga frågor* 135
9.1 Köp och hemförsäljning, m.m. 135
9.2 EDI inom tillverkningsindustrin 136
9.3 EDI inom offentlig upphandling 137

Avdelning III
Elektroniska förmedlingstjänster

10 *Utgångspunkter* 141
10.1 Vad är en elektronisk förmedlingstjänst? 141
10.1.1 Allmänt 141
10.1.2 Teknik, m.m. 142
10.1.3 Terminologi och användningssätt 143
10.2 Vilka rättsfrågor framträder 147
10.2.1 Straffrättsliga frågor 147
10.2.2 Straffprocessuella frågor 152
10.2.3 Skyddet mot otillbörligt integritetsintrång 154
10.2.4 Arkivering — gallring 156
10.2.5 Sekretess 156
10.2.6 Grundlagsfrågor, m.m. 157

11 *Överväganden* 163
11.1 Utgångspunkter 163
11.2 Anpassningar för att undanröja hinder mot ett fritt meningsutbyte 164
11.2.1 Skyddet för persondata 164
11.2.2 Undantag för löpande text, m.m. 165

11.2.3 Förhållandet till dataskyddsdirektivet 168
11.2.4 Personligt bruk 169
11.3 Regler till skydd mot missbruk 170
11.3.1 Bör en särskild reglering införas? 170
11.3.2 Vilka tjänster bör omfattas av en reglering? ... 173
11.3.3 Vem bör en reglering riktas mot? 174
11.3.4 Lagstiftningstekniken 175
11.3.5 Närmare om den särskilda lagens tillämpningsområde 176
11.4 Regleringens huvudsakliga innehåll 177
11.4.1 Allmänt 177
11.4.2 Vilka förmedlingstjänster avses 177
11.4.3 Registrering av förmedlingstjänster eller andra åtgärder för att peka ut en ansvarig? 179
11.4.4 Vem bör regleringen riktas mot 180
11.4.5 E-post och slutna grupper 182
11.4.6 Ansvarets närmare innebörd 183
11.4.7 Registrering och uteslutning av användare? ... 185
11.4.8 En skyldighet att informera 186
11.4.9 Straffansvar, förverkande och skadestånd 188
11.5 Tillsyn 190
11.6 Konkurrerande regler i datalagen, telelagen och den särskilda lagen 191
11.7 Nationella begränsningar 192
11.8 Åtgärder i andra länder 194
11.9 Offentlighetsinsynen och de elektroniska förmedlingstjänsterna 194

12 *Straffrättsliga och straffprocessuella frågor* 197
12.1 Utgångspunkter 197
12.2 Ansvar för användare vid missbruk av elektroniska förmedlingstjänster 198
12.2.1 Uppvigling, hets mot folkgrupp, barnpornografibrott, m.m. 198
12.2.2 Ansvar enligt brottsbalken för brott mot en viss person 200
12.2.3 Narkotikabrott genom utbud via elektroniska förmedlingstjänster 201
12.2.4 Skadegörande programkod, m.m. 201
12.2.5 Upphovsrättsligt skydd 202
12.2.6 Meddelanden vilkas innehåll är ägnat att användas vid brott 202
12.3 Straffansvar för den som tillhandahåller en elektronisk förmedlingstjänst 203
12.3.1 Allmänt 203

12.3.2 Tillämpningen av enskilda straffbestämmelser . . 204
12.3.3 Skyldigheter för den som tillhandahåller tjänsten och skyddet mot intrång i information, m.m. . . 206
12.4 Processrättsliga frågor 208
12.4.1 Bakgrund 208
12.4.2 Är allmänt tillgängliga förmedlingstjänster tillgängliga för polisen? 209
12.4.3 Brottsliga förfaranden vid spaning och utredning? 210
12.5 Konsekvenser av mina förslag 211

Särskilda yttranden 215
Av experten Göran Axelsson 215
Av experten Ingela Halvorsen 217

Bilagor

Bilaga 1 Direktiven 219
Bilaga 2 Informationssäkerhet 231
Bilaga 3 Arkiv — bevarande och gallring 241
Bilaga 4 Rättsliga "standarder" 249
Bilaga 5 Elektronisk adressering, postöppning och diarieföring 251
Bilaga 6 Elektroniska akter, m.m. 255
Bilaga 7 Förvaltningslagen och IT 265

Förkortningar

ADB	Automatisk databehandling
AvtL	Lagen (1915:218) om avtal och andra rättshandlingar på förmögenhetsrättens område
BrB	Brottsbalken
DelgL	Delgivningslagen (1970:428)
Dir.	Direktiv
DL	Datalagen (1973:289)
Ds	Departementsserien
EG	Europeiska gemenskaperna
E-post	Elektronisk post
EDI	Electronic Data Interchange
EU	Europeiska unionen
FL	Förvaltningslagen (1986:223)
FPL	Förvaltningsprocesslagen (1971:291)
HD	Högsta domstolen
ISO	Internationella standardiseringsorganisationen
IT	Informationsteknik
NJA	Nytt Juridiskt Arkiv, avdelning I
NJA II	Nytt Juridiskt Arkiv, avdelning II
Prop.	Proposition
RB	Rättegångsbalken
RF	Regeringsformen
RH	Rättsfall från hovrätterna
RÅ	Regeringsrättens årsbok
SIS	Standardiseringsorganisationen i Sverige
SOU	Statens offentliga utredningar
TF	Tryckfrihetsförordningen
YGL	Yttrandefrihetsgrundlagen

Sammanfattning

Mitt uppdrag har varit att utarbeta de förslag till rättslig reglering som kan behövas när elektroniska dokument och tjänster för förmedling av elektroniska meddelanden skall ersätta traditionella rutiner. Bakgrunden är dels myndigheternas och näringslivets strävanden att rationalisera verksamheter med stöd av den moderna informationstekniken (IT), dels den snabba utvecklingen av nya tjänster för förmedling av elektroniska meddelanden.

Beträffande frågan om *myndigheternas dokumenthantering* har jag i huvudsak kunnat bygga vidare på de synsätt som legat till grund för införandet av elektroniska dokument på bl.a. tull- och skatteområdena, samt de förslag som lagts fram till IT-anpassning av brotten mot urkunder. Till att börja med föreslår jag att definitioner av begreppen elektronisk handling, digitalt dokument, digital signatur och digital stämpel förs in i förvaltningslagen. Genom en användning av digitala signaturer och stämplar kan nämligen rättsregler skrivna för traditionell pappersbaserad uppgiftshantering — med endast smärre justeringar — tillämpas också i IT-miljö, utan att de allmänna principerna för en rättssäker ärendehandläggning behöver rubbas. För de fall där en förfaranderegel i lag, om handläggning av förvaltningsärenden, föreskriver något som medför att elektronisk dokumenthantering inte kan användas — t.ex. att handlingar skall vara egenhändigt undertecknade — föreslår jag en bestämmelse om att regeringen får föreskriva att digitala dokument eller, när det kan anses tillräckligt, elektroniska handlingar utan digital signatur eller stämpel får användas.

Jag tar vidare upp vissa praktiska frågor med anledning av den snabba övergången till elektronisk post, och föreslår nya bestämmelser dels i rättegångsbalken, förvaltningsprocesslagen och förvaltningslagen om inkommande elektroniska handlingar, dels i delgivningslagen om elektroniskt överbringande av handlingar.

Beträffande inkommande handlingar föreslås den huvudregeln att handlingar som överförs elektroniskt skall anses ha kommit in när data som representerar handlingen har nått myndighetens tekniska funktion för att ta emot e-post. Detta avses gälla oberoende av om denna funktion är placerad direkt i myndighetens informationssystem eller om ett förmedlingsföretag tillhandahåller tjänsten så att "brevlådan" finns hos förmedlaren. Bestämmelserna kompletteras med vissa undantagsregler som i huvudsak motsvarar gällande rätt, samt med föreskrifter

om rätt för myndigheter att anlita annan för teknisk bearbetning av elektroniska handlingar så att de kan läsas eller annars uppfattas.

Reglerna i delgivningslagen byggs ut med bestämmelser om ordinär delgivning samt förenklad delgivning genom elektronisk överföring till den sökte. Tillämpningsområdet föreslås emellertid bli begränsat för att undvika risker för rättsförluster för enskilda och det allmänna. Jag föreslår bl.a. att vare sig elektronisk delgivning eller förenklad elektronisk delgivning skall få avse stämningsansökningar eller andra handlingar genom vilka förfarandet vid myndigheten inleds och att förenklad elektronisk delgivning skall få användas endast om myndigheten genom ett tekniskt förfarande (kvittens) underrättas när handlingen har nått den söktes elektroniska adress.

Slutligen föreslår jag beträffande myndigheternas dokumenthantering en ändring i datalagen, för att anpassa den registrerades rätt att få s.k. 10 § - utdrag till användningen av elektroniska akter, samt en ändring i sekretesslagen, för att säkerställa att hemliga nycklar som myndigheter använder endast för digital signering kan skyddas mot insyn.

Beträffande *näringslivets användning av digitala dokument* har min genomgång visat att nuvarande civilrättsliga reglering i huvudsak bör kunna fungera också med avseende på elektronisk handel. Därför föreslår jag endast den ändringen att frågan om vem som står risken för att ett meddelande förvanskas under befordran skall regleras på samma sätt som när en handling försenas eller inte kommer fram (40 § avtalslagen).

Vad slutligen beträffar frågan om behovet av en reglering av *s.k. elektroniska anslagstavlor* föreslår jag en särskild lag med vissa undantag från datalagen — och därmed från EG:s dataskyddsdirektiv — så att ett fritt meningsutbyte inte hindras. Vidare föreslår jag bestämmelser i den särskilda lagen för att hindra missbruk av sådana elektroniska förmedlingstjänster. Eftersom den användare som ligger bakom ett missbruk ofta inte kan återfinnas till följd av utformningen av de tekniska och administrativa rutinerna i anknytning till elektroniska förmedlingstjänster, föreslår jag att den som tillhandahåller en tjänst för förmedling av elektroniska meddelanden skall informera om bl.a. vem som tillhandahåller tjänsten samt ha uppsikt över den. För vissa fall föreslår jag också en skyldighet att förhindra fortsatt spridning av meddelanden, och att denna skyldighet samt den nämnda skyldigheten att informera användarna straffsanktioneras. Slutligen föreslår jag en bestämmelse om att datorer och andra hjälpmedel som har använts vid brott enligt den föreslagna lagen skall få förklaras förverkade, om åtgärden behövs för att förebygga brott eller det annars finns särskilda skäl.

Summary

Background

This report presents the findings of a governmental committee, established to examine the need for change to existing laws in the area of data transmission to accommodate new requirements in society. The committee´s mandate was to consider suggestions for the legal redefinitions that are necessitated by the replacement of traditional and established routines of document transmittal and verification by electronic documents and services. Rapid changes are occurring in the area of Information Technology (IT), and difficulties arise when one attempts to integrate modern computing and telecommunication techniques into the current legal structure. Traditional boundaries existing between e.g. various forms of media and geo-political entities are easily and effectively penetrated.

The primary reasons for the enquiry originated from two distinct sources: The perceived need by governmental authorities and the private sector to improve the efficiency of their operations through the utilization of modern IT; and the rapid development of innovative services and technologies used in the mediation and transportation of electronic messages. With these factors in mind, the findings of the committee may be divided into three separate parts.

The first of these deals with governmental authorities´ management of documents and the obstacles to the utilization of IT in administrative functions (Chapters II-VI). Questions are dealt with that arise when documents of a traditional nature are replaced by digital "equivalents". Among other things, there are suggested definitions of digital documents and the like, as well as rules concerning the receipt of electronic documents and the electronic serving of documents.

The second part addresses questions relating to civil law as it pertains to the management of electronic documentation (Chapters VII-IX). The suggestion is made that most questions that arise in this area can be answered within the framework of current contractual law.

Finally, questions regarding Bulletin Board Systems and similar electronic services are presented (Chapters X-XII). A recommendation for a law focused on suppliers of such services is presented in the report.

Proposals of the committee

Administrative procedure

Swedish public administration is extensively computerized. However, the main body of legislation in this area was established in the 1970's, when e.g. the Swedish Data Act and provisions in the Swedish Constitution concerning public electronic records were introduced. While it is true that the Swedish Administrative Procedure Act, introduced in the 1980's, has been designed to provide legal principles applicable to paperbased as well as electronic handling of cases, the relevant legislation as a whole reflects a view of computers and databases which now must be viewed as antiquated.

Swedish legislative work concerning documents with digital signatures began in 1989 with new regulations for customs procedures. The legislator observed the possibility of combining legal requirements with the principles behind international standardization concerning digital signatures and related services, as well as creating a base for a legally unified regulation of paperbased and electronically administered routines.

In principle, this present committee has been able to build upon the legislation that has previously been introduced in such areas as customs procedures. The fundamental idea is to have digital signatures or their equivalents as substitutes for the verification characteristics in a paper document. A basic assumption has been that the digital document needs to provide the same evidence as a paper document, and must be able to be linked to a specified originator.[1] Therefore, the password method has not been accepted. Definitions have instead been based upon the need for verification of the documents themselves. — The committee has also presented a definition of records that lack inherent protection with regards to their authenticity.[2]

Given these definitions, it has been natural to solve the various legal questions that arise on the basis of the rules which are already established for paper documents. Questions concerning legal difficulties

[1] From a legal viewpoint, it was felt that technical descriptions should be avoided. In the establishment of laws, more abstract formulations could be used where the foundational functions are contained, and at the same time clarify the demand for verification both for the originator and the contents.

[2] *electronic record*: a defined set of data, which can be viewed, listened to or otherwise apprehended only by electronic means,

digital document: an electronic record with a digital signature or a digital stamp,

digital signature: the result of a transformation of an electronic record, by means of a unique key, making it possible to ascertain if the contents originate from the individual designated as issuer.

digital stamp: the result of a transformation of an electronic record, by means of a unique key, making it possible to ascertain if the contents originate from the legal person or authority designated as issuer.

which arise from digital documents and signatures are thereby replaced by the possibility to create a legally unified regulation of traditional routines and IT-routines. The functions of a paper document are then replicated within the framework of useful applications of a digital signature, with security maintained and without the general principles of legal procedure being affected.[3]

The committee also addresses *certain practical questions* arising due to the rapid transition to electronic document handling and E-mail.

If the relevant act, in a case involving legal procedures, prescribes something which precludes the usage of electronic document transmission, such as the requirement of a handwritten signature, the committee recommends that the government be allowed to stipulate that digital documents (or, if that is deemed to be sufficient, electronic records without a digital signature or stamp) may be used.

Also suggested by the committee are new provisions concerning the establishment of the point in time when incoming electronic records are deemed to have been received by an agency. In a traditional environment, a document is deemed to have been received by an agency the day upon which the document is delivered to the agency. This rule may also be applied when a diskette is mailed via the postal service to an agency.

In those cases where messages are transmitted via an electronic network, the principle applied is that the document is deemed to have been received by the agency when the data which represents the document have reached the agency's mail-receiving function. This is seen as being applicable whether this receiving function is physically located in the agency's information system or has been relegated to a mediating company which furnishes a service in which the "mailbox" is physically located on the mediating company's premises. These provisions are complemented by certain stipulated exceptions which primarily correspond to current legal practice.[4]

Also recommended is a right for agencies to require confirmation by the originator when a message lacks the originator's handwritten signature, as well as to commission a third party for the technical conversion of electronic documents so that they may be read or otherwise comprehended.

[3] The attainment of a sufficient level of security has been judged as being primarily a technical problem, with the presuppositions that both the contents and the originator should be possible to be verified — as when the demands of a digital signature according to ISO-standards are fulfilled.

[4] A document that is transmitted electronically is deemed to have arrived to an agency that day when the document

1. has arrived to the agencies electronic address,
2. has been received by a qualified employee, or
3. may be assumed to have arrived to the agencies electronic address, if it has come into the hands of a qualified employee the following working day.

The committee also suggests additional regulations regarding the serving of documents electronically, i.e. how to ascertain proper receipt of electronically transmitted documents. Present regulations concerning the serving of documents are enhanced with stipulations on "ordinary electronic serving" and "simplified electronic serving". The committee recommends, however, that areas of application be limited in order to avoid the risk of loss of legal rights. The rules on "electronic serving" shall not pertain to applications for a summons or other documents through which proceedings are initiated. Also, the "simplified electronic serving" shall be used only if the agency through a technical process (delivery notification) is informed when the document has reached the served party's electronic address.

Under section 10 of the Data Act (1973:289), an individual has the right to, if he so requests, be informed about the information on himself in personal files kept by an agency or a private company. A regulation, that limits an agency's need to give such information kept in electronic case files, is suggested.

Finally, the committee deals with the need in an IT environment for orderliness, e.g. concerning archival processing including registration and filing of incoming E-Mail. No new legislation is required in this regard. However, when an agency establishes routines for electronic message handling and the like, it is important that these procedures fulfill the applicable requirements.

Electronic document handling in the private sector

The increased demand within the private sector for effectivity has resulted in the use of IT not being limited to the conversion of traditional routines to their electronic equivalents. Instead, the entire pattern of commerce is transformed,[5] and the focus of change becomes automatic *processes*, rather than *products* such as bids, contracts, invoices, bills of lading, etc. Striving to utilize the entire potential for rationalization that IT offers has led to a balancing between effectivity and security that, in some cases, may need to be reevaluated.

The private sector has attempted to solve the legal questions that arise by constructing model contracts on how contracts should be entered into, such as the so-called EDI agreements. Among other things, these contracts deal with questions that arise when involved parties enter into agreements automatically, i.e. when computers generate and transmit messages that result in a binding agreement. Electronic commerce will most likely, at least in certain areas, attain

[5] Examples of this are the concept "Just in Time" and "Business Process Reengineering", where even such demands that have been perceived as obvious from a legal point of view may be questioned.

such dimensions that it will hardly be possible to initiate and preserve written EDI agreements with every business associate. Therefore, there is a need for a functioning legal structure even within civil law concerning the creation of predictable and secure information in electronic contract formulations.

The committee has nevertheless found that most of the questions that arise may be answered within the framework of current contractual law. Not every detailed question can be answered in advance, but contract law is commonly kept and is limited to general principles which are appropriate for agreements of varying type. Questions that do not directly fit under any of the prevailing regulations should still be able to be dealt with in close relation to the principles upon which contract law is based.

Regarding the question of whether or not electronic manifestations of a party's "will", generated automatically without direct human involvement, can result in binding contracts, a parallel can be drawn with such traditional "mass" transactions that occur frequently and in large volume in daily practice. Typical contracts that fall into this group are simple, small purchases in stores or a bus trip paid in cash. It may also be cited from Swedish jurisprudence that a contract regarding parking is deemed to be entered into by simply placing the car in a parking place.

In a similar manner, the individual that electronically and automatically makes an offer or an acceptance is bound by the offer or reply. The purpose of the entire procedure is to create binding agreements when certain exterior circumstances combined with one another function as the direct establishment of a contract. The legal text is sufficiently accommodating to allow a non-prejudicial application of contract law, while at the same time avoiding a new construction that departs from traditional civil law.

However, certain provisions in contract law lose their purpose when contracts are entered into completely automatically. These are the provisions that presuppose human behavior patterns, such as those dealing with coercion, deceit and usury. A computer, for example, cannot threaten another computer. However, this does not necessitate any amendments in contract law since irrational results may be corrected through the so-called general clause, which is completely free from subjectivity.

Also in other areas current contract law should be applicable to the IT area. For example, this is true concerning provisions regarding liability because a transmitted message is delayed or never received, as well as provisions dealing with "written" and "oral" communication.

The committee suggests, however, an amendment in contract law concerning the question of who is liable when an electronic message has been corrupted during transmission. A complementary addition to

the current provisions concerning assignment of risk due to the delay or disappearance of a message is recommended. This provision should also be applicable when a message is corrupted during transmission to the receiver (Section 40 of the Contract Law). The Contract Law will then correspond to the present Law of Contract of Sale of Goods, which came into force in 1990.

Bulletin Board Systems and similar computer mediated communication services

The usage of computers and telecommunication has meant increased possibilities to simply and inexpensively spread information via Bulletin Board Systems (BBS), whereby user groups can post their own messages and read those from others. Development is progressing rapidly, however, and the phrase BBS is already somewhat antiquated. With regards to Bulletin Boards and similar services that are offered via e.g. the Internet, the committee´s suggestion is presented in the form of an Electronic Mediation Services Bill.

Through such mediation services, there are created new possibilities to communicate, irrespective of geographical location. One purpose of the new legislation is to remove hindrances to such communication. Therefore, exceptions are suggested to the Data Act (1973:289) to enable users to deposit or collect information enabling free exchange of opinions, free and comprehensive information and freedom of artistic creation. This section is related to article 9 of the European Communities directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

However, the electronic mediation services have also opened up avenues for crime. Ordinarily a person who posts to a mediation service e.g. a copyrighted work or a racist statement can not be traced. The same is true of one who downloads this type of message to his computer. Therefore, certain regulations are suggested to focus on the person who supplies such services, in order to reduce the risks of abuse. The question becomes what responsibility should be borne by the service supplier.

Discussions during the period of inquiry have shown that the injunction upon the supplier of an electronic mediation service must be relatively limited, if the free exchange of information is not to be hindered. The reason for this is that the volume of information distributed via electronic mediation services, independent of time and space, is so large that it cannot be read or otherwise controlled by the service supplier. The expense involved in initiating such a function would prove to be prohibitive. For similar reasons there is not proposed any obligation to preserve the messages that are transmitted. The committee has only suggested an unsanctioned provision stating that the

person who provides the service should have the degree of supervision over the service that is necessary with regards to the scope and aims of the operation.

However, there is proposed an obligation upon the service supplier to inform everyone who wishes to utilize the service as to (a) who provides it, (b) the user's responsibility for the content of the electronic messages submitted and (c) to what degree received messages will be available to other users. Failure to give this information would be a criminal offence.

Also proposed is an obligation upon the service supplier to hinder further distribution of an electronic message if it is obvious that a user, by posting the message, has made himself liable to a crime, that infringement of copyright is taking place, or that the contents of a message are liable to be used in crime. This responsibility is shared by any person who is commissioned by the service supplier to supervise the service. Failure to hinder further distribution of such messages would be a criminal offence. If a crime exists, then the computer and other system components may be declared forfeit.

However, criminal liability is proposed to be present only if criminal intent exists. In practice, this means that the responsibility to hinder further distribution is imposed only if the responsible party is aware of the message and its character.

Consequently, no demands are placed upon the service supplier to be aware of all the information that is mediated. Instead, the idea is that the proposed obligation to hinder further distribution of unacceptable messages will carry with it a self regulation of the area.

The committee has also analysed certain questions of criminal law. Current penal regulations can in all respects be applied also to criminal conduct via a network. Although the perpetrator may be difficult to trace, the service supplier is — through the proposed legislation — given such a position that he, in certain circumstances, may be judged responsible as an accessory to the users crime according to the Swedish Penal Code, if the service supplier passively watches when a user carries on a criminal activity via the mediation service.

Certain questions of criminal procedure have also been addressed.[6] In this case, however, such questions of principle and general applicability have arisen that it has not been possible to deal with them in this limited context. A difficulty that should be mentioned, however, is how investigation and criminal inquiry can take place in cyberspace.

The proposed new legislation can in practice be applied only to activities which involve Sweden. Swedish police can naturally not act

[6] Cf the Council of Europe, Recommendation No. R (95) 13 of the Committee of Ministers to Member States Concerning Problems of Criminal Procedure Law Connected with Information Technology.

as a sort of international police force in the area of Bulletin Boards. Specific laws are not proposed in this section, but these questions must be solved in accordance with the general restrictions that apply in the area.

Considering the steps that are now being taken in other countries regarding Bulletin Boards and similar services, the Electronic Mediation Services Bill is presented below.

Electronic Mediation Services Bill

Areas of application

1 § This law applies to services that are intended for the electronic mediation of messages.

The law does not apply to:

1. the provision alone of a network or other connections for the transmission of messages,

2. mediation of messages within an agency or between agencies or within an enterprise or a legal group of enterprises, and

3. such services that are covered by the regulations in the Freedom of the Press Act or the Fundamental Law on Freedom of Expression.

In the law, "messages" means text, images, sounds and other information being transmitted in electronic form.

Exceptions from the Data Act

2 § The provisions in Sections 1-20 and 22-25 of the Data Act (1973:289) shall not be applied to personal registers that are maintained by a service according to this law, to the extent that

1. the registers contain only regular running text and information about messages and users of the service, and

2. the register is maintained for the purpose of enabling users to deposit or collect information with a view to free exchange of opinions, free and comprehensive information and freedom of artistic creation.

In the law, "regular running text" means information that has not been structured to facilitate the acquisition of personal information.

An overview of the service

3 § The service supplier shall have supervision over the service to the degree necessary with regards to the scope and aim of the operation.

Information to the user

4 § The service supplier shall, as soon as possible, inform each person who wishes to use the service about

1. who is supplying the service,
2. that the users are responsible for the content of the messages that they post, and
3. to what extent incoming messages become available to other users.

If an agency supplies the service it should also mention that messages which are mediated may become public documents.

The hinderance of continued distribution

5 § If it is obvious that a user, by posting a message, has made himself guilty of a crime or infringement of copyright or that the contents of the message are liable to be used in crime, the service supplier shall hinder further distribution of the message. The same applies to any person who supervises the service on behalf of the service supplier.

The first paragraph is not in effect if the message is intended to be received only by one or more designated recipients (electronic mail).

Penalties

6 § A person who intentionally or through negligence violates 4 § or who intentionally violates 5 § shall be sentenced to pay a fine or to imprisonment for at most six months, or, if the crime is serious, to imprisonment for at most two years. If the offence is of only a minor nature the offender shall not be sentenced.

The first paragraph is not applied if the offence is punishable under the Penal Code.

Forfeiture

7 § Computers and other equipment that have been used in a crime under this law may be declared forfeited, if this is called for in order to prevent crime or for other special reasons.

This law comes into force on ...

Författningsförslag

1 Förslag till lag om elektroniska förmedlingstjänster

Härigenom föreskrivs följande.

Tillämpningsområde

1 § Denna lag gäller tjänster som avser elektronisk förmedling av meddelanden.

Lagen gäller dock inte

1. tillhandahållande endast av nät eller andra förbindelser för överföring av meddelanden,

2. förmedling av meddelanden inom en myndighet eller mellan myndigheter eller inom ett företag eller en koncern, och

3. sådana tjänster som omfattas av regleringen i tryckfrihetsförordningen eller yttrandefrihetsgrundlagen.

I lagen avses med meddelanden text, bild, ljud eller information i övrigt som förmedlas i elektronisk form.

Undantag från datalagen

2 § Bestämmelserna i 1-20 och 22-25 §§ datalagen (1973:289) skall inte tillämpas på personregister som ingår i en tjänst enligt denna lag, i den mån

1. registret innehåller bara löpande text och uppgifter om meddelanden och användare, och

2. registret förs för att användarna skall kunna lämna eller inhämta uppgifter för ett fritt meningsutbyte, en fri och allsidig upplysning eller ett fritt konstnärligt skapande.

Med löpande text avses information som inte har strukturerats så att sökning av personuppgifter underlättas.

Uppsikt över tjänsten

3 § Den som tillhandahåller tjänsten skall ha sådan uppsikt över tjänsten som är nödvändig med hänsyn till omfattningen och inriktningen av verksamheten.

Information till användarna

4 § Den som tillhandahåller tjänsten skall så snart det kan ske underrätta var och en som vill använda tjänsten om

1. vem som tillhandahåller tjänsten,
2. att användaren är ansvarig för innehållet i de meddelanden han sänder in, och
3. i vilken utsträckning inkomna meddelanden blir tillgängliga för andra användare.

Om en myndighet tillhandahåller tjänsten skall den också ange att meddelanden som förmedlas kan bli allmänna handlingar.

Förhindrande av fortsatt spridning

5 § Om det är uppenbart att en användare genom att sända in ett meddelande har gjort sig skyldig till brott eller intrång i upphovsrätt eller att innehållet i ett meddelande är ägnat att användas vid brott, skall den som tillhandahåller tjänsten förhindra fortsatt spridning av meddelandet. Detsamma gäller den som på hans uppdrag har uppsikt över tjänsten.

Första stycket tillämpas inte om meddelandet är avsett bara för viss eller vissa mottagare (elektronisk post).

Straff

6 § Den som uppsåtligen eller av oaktsamhet bryter mot 4 § eller som uppsåtligen bryter mot 5 § döms till böter eller fängelse i högst sex månader eller, om brottet är grovt, till fängelse i högst två år. I ringa fall skall inte dömas till ansvar.

Första stycket tillämpas inte om det kan dömas till ansvar enligt brottsbalken.

Förverkande

7 § Datorer och andra hjälpmedel som har använts vid brott enligt denna lag får förklaras förverkade, om åtgärden behövs för att förebygga brott eller det annars finns särskilda skäl.

Denna lag träder i kraft den ...

2 Förslag till lag om ändring i brottsbalken

Härigenom föreskrivs att det i brottsbalken skall föras in en ny paragraf, 16 kap. 17 a §, av följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
	16 kap.
	17 a §
	Den som sänder ett elektroniskt meddelande med sådant innehåll som avses i 5, 8, 10 a, 10 b eller 12 § till en tjänst som omfattas av lagen (1997:000) om elektroniska förmedlingstjänster, med uppsåt att utföra brott som sägs i någon av dessa bestämmelser, skall dömas för försök till sådant brott enligt vad som föreskrivs i 23 kap. 1 § andra stycket, om han inte kan dömas för fullbordat brott.

Denna lag träder i kraft den ...

3 Förslag till lag om ändring i rättegångsbalken

Härigenom föreskrivs i fråga om rättegångsbalken

dels att 33 kap. 3 § skall ha följande lydelse,

dels att det i balken skall föras in tre nya paragrafer, 33 kap. 3 a, 3 b och 9 a §§, av följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
	33 kap.
	3 §
En handling anses ha kommit in till rätten den dag då handlingen eller en avi om betald postförsändelse som innehåller handlingen anlänt till rätten eller kommit en behörig tjänsteman till handa. Underrättas rätten särskilt om att ett meddelande till rätten anlänt till ett telebefordringsföretag, anses meddelandet ha kommit in redan när underrättelsen nått en behörig tjänsteman.	
Kan det antas att handlingen eller en avi om denna en viss dag har lämnats i rättens kansli eller avskilts för rätten på postanstalt, anses den ha kommit in den dagen, om den kommit en behörig tjänsteman till handa närmast följande arbetsdag.	
Om det behövs får rätten begära att ett telefax eller annat meddelande som saknar avsändarens underskrift i original bekräftas av avsändaren genom en i original undertecknad handling. Har rätten begärt en sådan bekräftelse men inte fått någon, får rätten bortse från meddelandet.	
	3 a §
	En handling som överförs elektroniskt anses ha kommit in till rätten den dag då handlingen
	1. har anlänt till rättens elektroniska adress,
	2. har tagits emot av en behörig tjänsteman, eller
	3. kan antas ha anlänt till rättens elektroniska adress, om

Nuvarande lydelse	*Föreslagen lydelse*
	den kommit en behörig tjänsteman till handa närmast följande arbetsdag.
	3 b §
	Om det behövs får rätten begära att ett meddelande som saknar avsändarens underskrift i original bekräftas av avsändaren genom en i original undertecknad handling. Har rätten begärt en sådan bekräftelse men inte fått någon, får rätten bortse från meddelandet.
	9 a §
	Rätten får vid behov låta tekniskt bearbeta en elektronisk handling som kommer in till eller skickas ut från rätten så att handlingen kan läsas eller annars uppfattas.
	Den som har biträtt rätten med den tekniska bearbetningen har rätt till skälig ersättning, som betalas av staten.

Denna lag träder i kraft den ...

4 Förslag till lag om ändring i lagen (1915:218) om avtal och andra rättshandlingar på förmögenhetsrättens område

Härigenom föreskrivs att 40 § lagen (1915:218) om avtal och andra rättshandlingar på förmögenhetsrättens område skall ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
40 §	
Skall någon enligt denna lag giva annan ett meddelande, vid äventyr att eljest avtal anses slutet eller anbud antaget eller rättshandling, som av honom eller å hans vägnar företagits, bliver mot honom gällande, och varder sådant meddelande inlämnat för befordran med post eller telegraf eller eljest på ändamålsenligt sätt avsänt, må ej den omständigheten, att meddelandet försenas eller icke kommer fram, föranleda därtill att avsändaren icke anses hava fullgjort vad honom åligger.	Skall någon enligt denna lag giva annan ett meddelande, vid äventyr att eljest avtal anses slutet eller anbud antaget eller rättshandling, som av honom eller å hans vägnar företagits, bliver mot honom gällande, och varder sådant meddelande inlämnat för befordran med post eller telegraf eller eljest på ändamålsenligt sätt avsänt, må ej den omständigheten, att meddelandet försenas, *förvanskas* eller icke kommer fram, föranleda därtill att avsändaren icke anses hava fullgjort vad honom åligger.

I fråga om återkallelse av anbud eller svar eller av fullmakt gäller vad i 7, 13 och 18 §§ är stadgat.

Denna lag träder i kraft den ...

5 Förslag till lag om ändring i delgivningslagen (1970:428)

Härigenom föreskrivs i fråga om delgivningslagen (1970:428)

dels att 3, 6 och 19 §§ skall ha följande lydelse,

dels att det i lagen skall föras in tre nya paragrafer, 1 a, 3 b och 3 c §§, av följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
	1 a §
	I denna lag har begreppen elektronisk handling, digital signatur och digital stämpel samma betydelse som i 1 a § förvaltningslagen (1986:223).
	3 §
Myndighet ombesörjer delgivning genom att sända handlingen med post eller överlämna den med bud eller på annat sätt till den sökte, varvid som bevis att denne har mottagit försändelsen begäres delgivningskvitto eller mottagningsbevis (ordinär delgivning). Ordinär delgivning kan också ske *genom förenklad delgivning enligt 3 a §.*	Myndighet ombesörjer delgivning genom att sända handlingen med post eller överlämna den med bud eller på annat sätt till den sökte, varvid som bevis att denne har mottagit försändelsen begäres delgivningskvitto eller mottagningsbevis (ordinär delgivning). Ordinär delgivning kan också ske *på de sätt som anges i 3 a - 3 c §§.*

Om det finns anledning antaga att delgivningskvitto eller mottagningsbevis ej kommer att lämnas eller ej kommer att erhållas i tid, får myndighet som regeringen bestämmer ombesörja att handlingen överlämnas till den sökte i särskild ordning genom postbefordringsföretag som regeringen bestämmer (särskild postdelgivning).

När det är lämpligt, får en myndighet delge kallelser, meddelanden och andra handlingar, som inte är omfattande eller annars av svårtillgängligt innehåll, genom att innehållet läses upp vid telefonsamtal med den sökte och handlingen därefter sänds till denne med post (telefondelgivning). Sådan delgivning får inte avse stämningsansökningar eller andra handlingar genom vilka förfarandet vid myndigheten inleds.

Nuvarande lydelse

Kan delgivning inte ske enligt första-tredje styckena, får delgivning ske genom stämningsman eller annan, vars intyg enligt 24 § första stycket utgör fullt bevis om delgivning (stämningsmannadelgivning).

I fall som avses i 15 och 16 §§ får delgivning ske genom kungörelse (kungörelsedelgivning).

Föreslagen lydelse

3 b §

När det är lämpligt, får ordinär delgivning ske genom att myndigheten överför en elektronisk handling till den sökte och begär bevis om att denne har mottagit handlingen (elektronisk delgivning).

Elektronisk delgivning får inte avse stämningsansökningar eller andra handlingar genom vilka förfarandet vid myndigheten inleds.

3 c §

När det är lämpligt, får ordinär delgivning med den som är part eller som har liknande ställning i ett mål eller ett ärende ske genom att myndigheten överför en elektronisk handling till den söktes elektroniska adress och minst en dag senare överför ett meddelande om den första överföringen (förenklad elektronisk delgivning).

Förenklad elektronisk delgivning får användas bara om

1. den sökte har delgetts upplysning om att förenklad elektronisk delgivning kan komma att användas i målet eller ärendet eller den sökte har inlett förfarandet vid myndigheten eller har gett in en handling i målet eller ärendet och sådan upplysning har sänts med post i nära anslutning

Nuvarande lydelse	*Föreslagen lydelse*
	till att ansökan eller handlingen har kommit in till myndigheten, *2. det i upplysningen enligt 1 har angetts till vilken elektronisk adress delgivning kan komma att ske,* *3. myndigheten genom ett tekniskt förfarande (kvittens) underrättas när handlingen och meddelandet om handlingen har nått den söktes elektroniska adress, och* *4. delgivningen inte avser en stämningsansökan eller en annan handling genom vilken förfarandet vid myndigheten inleds.*
6 §	
Vid delgivning överbringas handlingen i original eller styrkt kopia. En kopia som har framställts vid en myndighet behöver inte bestyrkas.	Vid delgivning överbringas handlingen i original eller styrkt kopia. En kopia som har framställts vid en myndighet behöver inte bestyrkas. *När det kan ske skall myndigheten förse elektroniska handlingar med digital signatur eller stämpel.*

Är handling som skall delges av vidlyftig beskaffenhet eller är det av annan anledning ej lämpligt att handlingen mångfaldigas, får myndigheten besluta, att handlingen i stället skall hållas tillgänglig hos myndigheten eller på plats, som myndigheten bestämmer. Meddelande därom och om den tid, under vilken handlingen hålles tillgänglig, delges den sökte.

Andra stycket gäller *ej* delgivning av stämningsansökan eller annan handling, *varigenom talan anhängiggöres.* I fråga om bilaga till sådan handling får andra stycket dock tillämpas.	Andra stycket gäller *inte* delgivning av stämningsansökan eller annan handling, *genom vilken förfarandet vid myndigheten inleds.* I fråga om bilaga till sådan handling får andra stycket dock tillämpas.

19 §

Delgivning har skett genom att den som söks för delgivning själv har mottagit handlingen, oavsett på vilket sätt den kommit honom till

Nuvarande lydelse *Föreslagen lydelse*

handa. Har den sökte kvitterat postförsändelse som hämtats av bud, skall den anses ha kommit honom till handa samma dag som den avhämtats av budet.

Förekommer vid särskild postdelgivning eller stämningsmannadelgivning att den som sökes för delgivning vägrar att taga emot handlingen, anses delgivning ändå ha skett.

Delgivning skall anses ha skett

enligt 6 § andra stycket genom att handlingen är tillgänglig och meddelandet delgivits,

enligt 3 a § när två veckor förflutit från det att meddelandet skickades med post och det inte med hänsyn till omständigheterna framstår som osannolikt att handlingen före tvåveckorstidens utgång kommit fram till den söktes senast kända adress,

enligt 3 c § när två veckor förflutit från det att myndigheten fått kvittenser på att handlingen och meddelandet om handlingen har nått den angivna elektroniska adressen,

enligt 3 § tredje stycket, 12 eller 13 § genom att det blivit fullgjort som föreskrivs där,

enligt 15 § andra stycket sista punkten genom att handlingen lämnats i den söktes hemvist eller fästs på dörren till hans bostad,

enligt 17 § på tionde dagen efter beslutet om kungörelsedelgivning under förutsättning att det blivit fullgjort som föreskrives i paragrafens första stycke.

Denna lag träder i kraft den ...

6 Förslag till lag om ändring i förvaltningsprocesslagen (1971:291)

Härigenom föreskrivs i fråga om förvaltningsprocesslagen (1971:291)

dels att 44 § skall ha följande lydelse,

dels att det i lagen skall föras in tre nya paragrafer, 44 a, 44 b och 52 a §§, av följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
44 §	
Handling anses ha kommit in till rätten den dag då handlingen eller avi om betald postförsändelse, i vilken handlingen är innesluten, anlänt till rätten eller kommit behörig tjänsteman till handa. Underrättas rätten särskilt om att telegram till rätten anlänt till telegrafanstalt, anses telegrammet ha kommit in redan när underrättelsen nått behörig tjänsteman.	
Kan det antas att handlingen eller avi om denna viss dag avlämnats i rättens kansli eller avskilts för rätten på postanstalt, anses den ha kommit in den dagen, om den kommit behörig tjänsteman tillhanda närmast följande arbetsdag.	
Telegram eller annat meddelande som icke är underskrivet skall bekräftas av avsändaren genom egenhändigt undertecknad handling, om rätten begär det.	
	44 a §
	En handling som överförs elektroniskt anses ha kommit in till rätten den dag då handlingen
	1. har anlänt till rättens elektroniska adress,
	2. har tagits emot av en behörig tjänsteman, eller
	3. kan antas ha anlänt till rättens elektroniska adress, om den kommit en behörig tjänsteman till handa närmast följande arbetsdag.

Nuvarande lydelse	*Föreslagen lydelse*
	44 b §
	Om det behövs får rätten begära att ett meddelande som saknar avsändarens underskrift i original bekräftas av avsändaren genom en i original undertecknad handling. Har rätten begärt en sådan bekräftelse men inte fått någon, får rätten bortse från meddelandet.
	52 a §
	Rätten får vid behov låta tekniskt bearbeta en elektronisk handling som kommer in till eller skickas ut från rätten så att handlingen kan läsas eller annars uppfattas.
	Den som har biträtt rätten med den tekniska bearbetningen har rätt till skälig ersättning, som betalas av staten.

Denna lag träder i kraft den ...

7 Förslag till lag om ändring i datalagen (1973:289)

Härigenom föreskrivs att det i datalagen (1973:289) skall föras in två nya paragrafer, 1 a och 10 a §§, av följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
	1 a §
	Bestämmelser om undantag från denna lag finns i lagen (1997:000) om elektroniska förmedlingstjänster.
	10 a §
	Uppgifter i handlingar som finns i en elektronisk akt vid en myndighet behöver inte tas med i ett registerutdrag enligt 10 § första stycket. Av registerutdraget skall dock framgå vilka handlingar som finns i en elektronisk akt som avser den registrerade.

Denna lag träder i kraft den ...

8 Förslag till lag om ändring i sekretesslagen (1980:100)

Härigenom föreskrivs att 5 kap. 3 § sekretesslagen (1980:100) skall ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
	5 kap.
	3 §
Sekretess gäller för uppgift som lämnar eller kan bidra till upplysning om chiffer, kod eller liknande metod som har till syfte att underlätta befordran eller användning i allmän verksamhet av uppgifter utan att föreskriven sekretess åsidosätts, om det kan antas att syftet med metoden motverkas om uppgiften röjs.	Sekretess gäller för uppgift som lämnar eller kan bidra till upplysning om chiffer, kod eller liknande metod som har till syfte att *1.* underlätta befordran eller användning i allmän verksamhet av uppgifter utan att föreskriven sekretess åsidosätts, *eller* *2. göra det möjligt att kontrollera om uppgifter har förvanskats,* om det kan antas att syftet med metoden motverkas om uppgiften röjs.

Sekretess gäller i verksamhet som avser förande av eller uttag ur körkortsregistret för uppgift om körkorts referensnummer, om det inte står klart att uppgiften kan röjas utan fara för att kontrollen av körkorts äkthet motverkas om uppgiften röjs.

Denna lag träder i kraft den ...

9 Förslag till lag om ändring i förvaltningslagen (1986:223)

Härigenom föreskrivs i fråga om förvaltningslagen (1986:223)

dels att 8 och 10 §§ skall ha följande lydelse,

dels att rubriken närmast före 1 § skall lyda "Tillämpningsområde och definitioner",

dels att det i lagen skall föras in fyra nya paragrafer, 1 a, 7 a, 10 a och 10 b §§, av följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
	1 a §
	I denna lag avses med
	elektronisk handling: en bestämd mängd data som kan läsas, avlyssnas eller på annat sätt uppfattas endast med tekniskt hjälpmedel,
	digitalt dokument: en elektronisk handling med digital signatur eller digital stämpel,
	digital signatur: resultatet av en omvandling av en elektronisk handling som gör det möjligt att kontrollera om innehållet härrör från den fysiska person som framstår som utställare, och
	digital stämpel: resultatet av en omvandling av en elektronisk handling som gör det möjligt att kontrollera om innehållet härrör från den juridiska person eller myndighet som framstår som utställare.
	7 a §
	Om en bestämmelse om handläggning av förvaltningsärenden i en annan lag föreskriver att handlingar skall vara egenhändigt undertecknade eller om den föreskriver något annat som med-

Nuvarande lydelse | *Föreslagen lydelse*

för att elektroniska handlingar inte kan användas, får regeringen föreskriva att digitala dokument eller, när det kan anses tillräckligt, elektroniska handlingar utan digital signatur eller stämpel får användas.

8 §

När en myndighet har att göra med någon som inte behärskar svenska eller som är allvarligt hörsel- eller talskadad, bör myndigheten vid behov anlita tolk.

En myndighet får vid behov låta tekniskt bearbeta en elektronisk handling som kommer in till eller skickas ut från myndigheten så att handlingen kan läsas eller annars uppfattas.

10 §

En handling anses komma in till en myndighet den dag då handlingen, eller en avi om en betald postförsändelse som innehåller handlingen, anländer till myndigheten eller kommer en behörig tjänsteman till handa. Underrättas en myndighet särskilt om att ett telegram till myndigheten finns hos ett företag som driver televerksamhet, anses telegrammet komma in redan när underrättelsen når en behörig tjänsteman.

Kan det antas att handlingen eller en avi om denna en viss dag har lämnats i myndighetens lokal eller avskilts för myndigheten på en postanstalt, anses den ha kommit in den dagen, om den kommer en behörig tjänsteman tillhanda närmast följande arbetsdag.

Ett telegram eller annat meddelande som inte är underskrivet skall bekräftas av avsändaren genom en egenhändigt undertecknad handling, om myndigheten begär det.

10 a §

En handling som överförs elektroniskt anses ha kommit in

Nuvarande lydelse	*Föreslagen lydelse*
	till en myndighet den dag då handlingen *1. har anlänt till myndighetens elektroniska adress,* *2. har tagits emot av en behörig tjänsteman, eller* *3. kan antas ha anlänt till myndighetens elektroniska adress, om den kommit en behörig tjänsteman till handa närmast följande arbetsdag.*
	10 b §
	Om det behövs får myndigheten begära att ett meddelande som saknar avsändarens underskrift i original bekräftas av avsändaren genom en i original undertecknad handling. Har myndigheten begärt en sådan bekräftelse men inte fått någon, får myndigheten bortse från meddelandet.

Denna lag träder i kraft den ...

1 Utredningsuppdraget och dess genomförande

Utredningens direktiv (dir. 1994:42) beslöts av regeringen den 19 maj 1994. De återges i sin helhet i *bilaga 1*. Av direktiven framgår att utredningen har till uppgift att utarbeta sådana förslag till rättslig reglering som kan behövas

— i samband med inrättandet av s.k. elektroniska anslagstavlor, och

— för användningen av elektroniska dokument inom förvaltningen och näringslivet.

Beträffande myndigheternas dokumenthantering har jag inriktat arbetet på sådana mer akuta rättsfrågor som den snabba förändringstakten för med sig för ärendehandläggningen. När det gäller näringslivets dokumenthantering har jag i huvudsak begränsat genomgången till det område som brukar kallas elektronisk handel.

Beträffande elektroniska anslagstavlor har jag låtit inhämta upplysningar från verksamma på IT-området om hur de nya kommunikationsvägarna används och vilka möjligheter som finns att överblicka och reglera dem. Under augusti 1995 har utredningen spritt en promemoria med förslag till reglering på området och med denna som underlag hållit en hearing med tekniker och administratörer samt en hearing med jurister.

Regeringen har till utredningen överlämnat en framställning från Umeå universitet med anledning av att pornografiska bilder spritts i universitetets datanät.

Jag har samrått med bl.a. kommittén angående nya medier och grundlagarna m.m. (dir. 1994:104) och kommittén angående ny datalag m.m. (dir. 1995:91).

Betänkandet har delats in i tre avdelningar.

Den *första avdelningen* (kap. 2-6) rör myndigheternas dokumenthantering, där bl.a. frågor om inkommande elektroniska handlingar och elektronisk delgivning behandlas.

Den *andra avdelningen* (kap. 7-9) avser civilrättsliga frågor med anknytning till elektronisk dokumenthantering.

Som en *tredje avdelning* (kap. 10-12) behandlas frågor om elektroniska anslagstavlor.

Dessutom behandlas i *bilagorna 2-7* vissa frågor som — utan att ha

föranlett några förslag till författningsändringar — är av betydelse för en fungerande och rättssäker övergång till elektronisk dokumenthantering. Där tas upp bl.a. frågor om informationssäkerhet, arkivering, rättsliga "standarder", elektronisk adressering och elektroniska akter.

Avdelning I
Elektronisk dokumenthantering i förvaltningen

2 Utgångspunkter

2.1 Inledning

Pappersbaserade handlingar har sedan mycket lång tid varit av stor betydelse i rättslivet och som instrument för kommunikation och handläggning inom bl.a. förvaltningen. Det har uppfattats som självklart att sådana handlingar avgränsar och bevarar uppgifter samt att det framgår vem som är utställare.[1]
Som exempel på sådana handlingar kan nämnas inlagor, deklarationer, protokoll och beslut. Det finns allmänt vedertagna rutiner för att sortera sådana handlingar, t.ex. i aktkappor eller pärmar, och handlingarna kan återsökas via dagboksblad, diarier och liknande förteckningar. Därigenom fogas handlingarna in i sitt rätta sammanhang. Dessa strukturer utgör en förutsättning för fungerande rutiner, där krav på bl.a. rättssäkerhet och intern och extern kontroll tillgodoses.

Dessa intressen kan tillgodoses också inom ramen för datorbaserade rutiner och det är angeläget att ta tillvara de möjligheter till rationaliseringar som den nya informationstekniken (IT) ger. Med IT avses här efterkrigstidens snabba utveckling av mer eller mindre integrerade system för automatisk databehandling (ADB) och telekommunikation, ibland kallade informationssystem. Det är nämligen inte längre möjligt att lägga tyngdpunkten på ADB, då i de nu snabbt framväxande informationssystemen kommunikationen av data är väl så betydelsefull som behandlingen av data.

Datoriseringen har i praktiken ofta fört med sig att uppgiftshanteringen anonymiserats och att strukturer och gränser utformats så att utrymmet för oklarheter blivit påtagligt. Rättsfrågor och frågor om informationssäkerhet har härvid fått stå tillbaka för krav på skyndsamma rationaliseringar. Nya dokumentrutiner har införts också för rättsligt och ekonomiskt betydelsefulla tillämpningar. Författningsregleringen och de tekniska lösningarna har emellertid endast delvis anpassats för en sådan IT-användning. Exempelvis har underskrivna pappersurkunder ersatts av elektroniska meddelanden utan motsvarande skydd mot

[1] De fysiska gränserna för löpande text och handlingar, där uppgifter på motsvarande sätt har strukturerats genom en användning av *blanketter*, uppfattas i traditionell miljö som underförstådda och självklara.

manipulationer, och det är oklart om skyddet enligt brottsbalken mot missbruk av urkunder är tillämpligt på data som överförs via nät.

Denna utveckling kan i viss mån förklaras genom ett studium av den uppgiftshantering för vilken datorerna först användes, nämligen sådana strukturerade samlingar av uppgifter — egentliga register — som tidigare fördes manuellt i form av t.ex. lösa kort sorterade i viss ordning eller böcker förda enligt liknande system.

När sådana uppgiftssamlingar används är det avgörande att uppgifterna är riktiga, medan användaren knappast bryr sig om vilka handläggare som har registrerat de enskilda uppgifterna. En avidentifiering sker därigenom så att uppgifternas ursprung från en viss individ ersätts av ett ursprung från ett visst informationssystem (jfr t.ex. uppgifterna i bilregistret med ett köpekontrakt).

2.2 Lagstiftning rörande elektroniska dokument, m.m.

De rättsfrågor som aktualiseras när traditionella urkunder ersätts av IT-baserade motsvarigheter har, som framgår av mina direktiv, redan varit föremål för lagstiftning på vissa områden. Riksdagen har beslutat om de författningsändringar som behövs för att ersätta pappersbaserade tulldeklarationer med elektroniska dokument.[2] I det lagstiftningsärendet uttalade konstitutionsutskottet att frågan om elektroniska dokument i förvaltningsförfarandet måste få en generell lösning.

Motsvarande reglering har införts för att göra det möjligt att ge in elektroniska ansökningar om registrering av datapantbrev enligt lagen (1994:448) om pantbrevsregister. Vid behandlingen av regeringens proposition 1993/94:197 om datapantbrev, anförde lagutskottet att regleringen beträffande elektroniska dokument kunde godtas i avvaktan på resultatet av de överväganden om en mer generell reglering av elektroniska dokument i förvaltningsförfarandet som kommer att ske (bet. 1993/94:LU33).[3]

Författningsändringar har också genomförts för att elektroniska dokument och akter skall kunna införas på skatteområdet[4] och inom exekutionsväsendet.[5] Ny var härvid frågan om de rättsliga konsekven-

[2] Prop. 1989/90:40, bet. 1989/90:KU2 och bet. 1990/91:KU11, se vidare SOU 1989:20.

[3] Jfr dock regleringen i t.ex. 9 § lagen (1990:746) om betalningsföreläggande och handräckning samt 6 - 8 §§ förordningen (1991:1339) om betalningsföreläggande och handräckning, med anknytande föreskrifter av Riksskatteverket, där det inte ställs krav på signering.

[4] Ds 1994:80, prop. 1994/95:93, bet. 1994/95:SkU15 och rskr. 1994/95:158.

[5] Finansdepartementets promemoria den 22 december 1994, Nytt ADB-stöd för indrivningsverksamheten, Fi94/2903, prop. 1994/95:168, bet. 1994/95:LU27 och rskr. 1994/95:305.

serna av en ärendehandläggning baserad på IT-baserade avbildningar av inkomna pappershandlingar.

Motsvarande frågor har, från straffrättslig och processuell utgångspunkt, behandlats av Datastraffrättsutredningen i betänkandet Information och den nya InformationsTeknologin — straff- och processrättsliga frågor (SOU 1992:110). Utredningens förslag övervägs inom Justitiedepartementet.

2.3 Utvecklingen i Sverige och internationellt

2.3.1 Den offentliga verksamheten i Sverige

Den offentliga verksamheten rationaliseras i allt högre takt. Internationaliseringen och samtidiga krav på service och besparingar leder till omprövning av åtaganden och arbetsuppgifter samt till omstrukturering av verksamheter och organisationer. Därvid blir åtgärder för att åstadkomma en fungerande, öppen och säker infrastruktur för informationsförsörjning av avgörande betydelse.

Investeringar i infrastruktur innefattar inte bara satsningar på IT. Företag och medborgare behöver enkla, likartade och säkra rutiner för sitt informationsutbyte, oavsett om detta utbyte sker med myndigheter eller företag.[6] Detta kan bli möjligt endast om allmänt accepterade förfaringssätt utvecklas. Härvid berörs nära nog varje rättsområde och behovet av att IT-anpassa författningsregleringen är uppenbart.

Myndigheter, kommuner och landsting har sökt nya former för samverkan eftersom sådana anpassningar inte är möjliga att åstadkomma på egen hand, och regeringen har tagit olika initiativ på området, bl.a. genom IT-kommissionen. Av särskilt intresse för mitt uppdrag är det arbetsprogram för förnyelse och effektivisering av offentlig verksamhet genom ökad användning av IT, som Finansdepartementet initierade våren 1994 — det s.k. Toppledarforum. Detta forum, som är en informell samverkansgrupp ledd av samordningsminister Jan Nygren[7], bedriver sin verksamhet i projekt. Syftet är att nå ett brett engagemang långt ut i verksamheterna. För närvarande är ett hundratal personer engagerade i projekten, som har inriktats på åtgärder som är generella och likartade för offentlig verksamhet, men som en myndighet inte rimligen kan vidta på egen hand.

Detta arbete väntas leda till att offentlig förvaltning mer samlat går över från pappersbaserad till elektroniskt stödd verksamhet. Det

[6] I USA uttrycks detta som "single face to industry" och "single face to citizen".

[7] Övriga ledamöter är ett tiotal generaldirektörer för informationsintensiva myndigheter samt cheferna för Landstingsförbundet och Svenska kommunförbundet.

planeras exempelvis att alla myndigheter senast år 1996 skall kunna ta emot och sända e-post och att den offentliga upphandlingen till övervägande del redan under år 1998 skall ske elektroniskt. Behovet av reglering rörande digitala dokument, digitala signaturer och anknytande rättsfrågor är alltså uppenbart.

Omfattningen av Toppledarforums arbetsprogram kan något förenklat anges genom följande sammanställning. Programmet innehåller tre huvuddelar. Den första huvuddelen, *Informationsförsörjning i offentlig förvaltning*, avser policyfrågor, rättsfrågor samt säkerhets- och kvalitetsfrågor, och innefattar två avslutade och två pågående projekt ("Prosit" och "Lexit" respektive "Offentliga organisationers internet-sidor" och "Qualit"). Den andra huvuddelen, *Informatikplattformar (standard, teknik, bastjänster)*, gäller åtgärder för att skapa förutsättningar för kommunikation "många-till-många" eller "alla-till-alla" för ärendebehandling och service till allmänhet och företag. I denna del bedrivs tre projekt ("E-post och katalog", "IT-plattformar" och "Smarta kort i offentlig verksamhet"). Den tredje huvuddelen, *Verksamhetsförnyelse i offentlig förvaltning med hjälp av IT*, avser gemensamma tillämpningsprojekt för många myndigheter vilka avses effektivisera informationsutbytet mellan offentlig förvaltning och företag, medborgare samt EU och andra internationella organ. I denna del bedrivs projektet "Elektronisk handel", som syftar till att införa elektroniska inköp i offentlig förvaltning.

Regeringen har i propositionen 1995/96:125 om åtgärder för att bredda och utveckla användningen av informationsteknik redovisat förslag till mål för en övergripande nationell IT-strategi som pekar ut Sveriges tilltänkta väg in i informations- och kunskapssamhället. I propositionen lämnas förslag till prioriterade statliga uppgifter — rättsordningen, utbildningen och samhällets informationsförsörjning — samt redovisas ett handlingsprogram för att bredda och utveckla användningen av informationsteknik.

2.3.2 Internationellt arbete

Sverige deltar i det arbete som pågår vid bl.a. EG-kommissionen, FN, UNCTAD, OECD och WIPO rörande digitala signaturer och elektronisk dokumenthantering i offentlig verksamhet. Arbetet inom EG-kommissionen är av särskild betydelse eftersom det kan antas påverka vår författningsreglering mer än annat internationellt samarbete. Som exempel kan nämnas det s.k. dataskyddsdirektivet (direktiv 95/46/EG av den 24 oktober 1995 om skydd för enskilda personer med avseende på behandlingen av personuppgifter och om det fria flödet av sådana

uppgifter), som antogs år 1995.[8] Ett annat betydelsefullt område är EG-kommissionens arbete med IT-säkerhet, där strävanden finns att skapa förutsättningar för elektronisk handel och elektronisk förvaltning. För att elektroniska rutiner inom elektronisk handel och förvaltning skall bli säkra från tekniska och rättsliga utgångspunkter behöver medlemsländerna komma överens om grunderna för dokumenthanteringen m.m.

Inom EU har många informationssystem tillskapats för att medlemsländernas förvaltningar skall kunna samverka och byta information i gemensamma ärenden. Behandlingen av dessa frågor har samordnas i det s.k. IDA-programmet (Interchange of Data between Administrations), som beslutades i november 1995. IDA-programmet väntas leda till rekommendationer och råd angående elektronisk dokumenthantering, rättsfrågor och IT-säkerhet. Dessutom planeras projekt för att genomföra sådana nya rutiner.

2.4 Uppdraget

Myndigheternas[9] användning av elektroniska dokument berör många olika rättsområden. Mitt uppdrag i denna del är dock i huvudsak begränsat till myndigheternas handläggning av mål och ärenden. Det är särskilt övergången till elektronisk kommunikation som här aktualiserar nya rättsfrågor.

Någon genomgripande revision av de berörda regelverken är inte avsedd och är inte heller lämplig i nuvarande läge. Vi befinner oss i ett intensivt utvecklingsskede, och det saknas fortfarande i väsentliga delar allmänt vedertagna synsätt. Det går därför inte att få en sådan detaljerad bild av de tekniska och rättsliga förutsättningarna som skulle krävas för genomgripande ändringar i regelsystemen. Till detta kommer att vissa frågor om t.ex. persondataskydd och offentlighetsinsyn övervägs i annan ordning.

[8] Direktivets tillämpningsområde är helt eller delvis automatisk behandling av personuppgifter och annan behandling än automatisk som ingår i eller kommer att ingå i ett register. Det gäller inte för behandling av personuppgifter som inte omfattas av gemenskapsrätten eller som rör en fysisk person som ett led i verksamhet av rent privat natur eller som har samband med hans hushåll. Något undantag för löpande text ges inte och varken elektroniska anslagstavlor eller nätverk nämns i själva direktivet. Tiden för införande av direktivet i nationell rätt är tre år för automatisk och 12 år för manuell behandling av personuppgifter.

Direktivets ändamål är att skapa en hög, för medlemsstaterna gemensam, skyddsnivå i fråga om behandling av personuppgifter. Härigenom kan ett fritt flöde av sådana uppgifter mellan staterna tillåtas. I ingressen framhålls att "skyddsnivån när det gäller enskilda personers fri- och rättigheter med avseende på behandlingen av sådana uppgifter (måste) vara likvärdig i alla medlemsstater". Det sägs därför vara nödvändigt att "gemenskapen vidtar åtgärder för att åstadkomma en tillnärmning till lagstiftningen".

[9] Med myndighet menas enligt regeringsformens (RF) terminologi samtliga statliga och kommunala organ, med undantag för riksdagen och de kommunala beslutande församlingarna. Andra myndigheter än domstolarna och regeringen kallas förvaltningsmyndigheter.

Uppgiften är i stället att tillgodose de akuta behoven av IT-anpassning av vissa rättsregler och att söka klarlägga hur vissa bestämmelser bör förstås när de skall tillämpas på nya rutiner. Det gäller att finna rättsliga lösningar och modeller som kan ge stöd för myndigheter som har infört eller står i begrepp att införa elektroniska rutiner.

2.5 Förslagets inriktning

Det finns enligt min mening inte några avgörande principiella invändningar mot att IT-rutiner jämställs med traditionella pappersbaserade rutiner vid myndigheternas ärendehandläggning. Det är t.o.m. möjligt att med hjälp av IT utforma ett mer likformigt och i vissa avseenden förutsebart förvaltningsförfarande än med motsvarande traditionella rutiner. IT kan också ge bättre insyn i myndigheternas verksamheter.

En förutsättning för att införa de nya rutinerna är emellertid att de tillgodoser behoven av bl.a. integritetsskydd och informationssäkerhet, rätten att ta del av allmänna handlingar och forskningens intressen samt ger grundläggande rättssäkerhetsgarantier. Här är skärpan i de tekniska och administrativa kraven av större betydelse än lagstiftningen. Det avgörande är att etablerade krav på rättssäkerhet, ordning osv. uppmärksammas på ett tidigt stadium när IT-rutiner införs, och att avsteg från kraven inte görs om inte befogade rättsskyddsintressen kan tas om hand på något annat, likvärdigt sätt. Jag behandlar sådana frågor om informationssäkerhet närmare i *bilaga 2*. De synpunkter som förs fram där är förutsättningen för de förslag om utökad IT-användning som jag lägger fram.

Vid en övergång till elektronisk dokumenthantering behöver det också övervägas hur långtidslagringen av dokument utformas. För att elektroniska handlingar skall kunna läsas många år senare behövs bl.a. upprepade läskontroller, konverteringar och överföringar till nya databärare, medan en äkthetsprövning på sikt av digitala dokument förutsätter en långsiktigt fungerande nyckelhantering. Det bör härvid betonas att god ordning och väl fungerande rutiner inom myndigheterna kan vara av lika stor betydelse som valet av teknik och systemlösningar. Om det inte tas hänsyn till de krav som måste ställas för ett långsiktigt bevarande av handlingar finns det risk för att informationen går förlorad, med de förluster som detta skulle innebära för såväl insynsintresset och det nationella kulturarvet som rättskipningen, förvaltningen och forskningen.[10]

Frågor om arkiv, bevarande och gallring m.m. behandlas närmare i avsnitt 6.4 och *bilaga 3*.

[10] Krav som syftar till en långsiktig läsbarhet av elektroniska handlingar finns i Riksarkivets regler angående ADB-upptagningar (RA-FS 1994:2 och 1994:7).

Det är vidare viktigt att myndigheternas tekniska hjälpmedel kan samverka med andra myndigheters eller enskildas informationssystem. Det vore olyckligt om varje myndighet för att godta elektroniska handlingar skulle uppställa egna långtgående krav på de tekniska rutinerna. Ett tillstånd av rättsosäkerhet och fara för rättsförluster skulle kunna uppkomma om enskilda inte vet om deras kommunikation med myndigheten i allmänt vedertagna former — vilka snabbt kan växla med hänsyn till utvecklingstakten inom IT — alls tillmäts någon betydelse. Det behövs således en samordning av myndigheternas arbete på IT-området, för att aktivt motverka oförenliga tekniska lösningar. Myndigheterna behöver härvid beakta företagens och enskildas intresse av att få lämna uppgifter på sätt som är anpassade till ingivarnas olika tekniska plattformar och olika datormognad.[11] Frågan om enhetliga lösningar är alltså betydelsefull från rättsliga utgångspunkter. Denna fråga behandlas vidare i *bilaga 4*.

I detta sammanhang vill jag också framhålla att övergången till elektronisk kommunikation enligt min mening i princip bör vara frivillig.

Enskilda har inte rätt att kräva att få sända meddelanden via telex eller elektronisk post till en myndighet som saknar tekniska hjälpmedel för att ta emot sådana meddelanden. Detsamma gäller om någon myndighet skulle sakna telefax. Jag föreslår ingen ändring i denna del; jfr 5 § första meningen förvaltningslagen (1986:223; FL). Det finns emellertid en allmän strävan att myndigheterna, för att rationalisera och erbjuda en bättre service, skall göra det möjligt att kommunicera med modern teknik. Denna strävan måste dock anpassas till vad som är genomförbart i varje enskilt fall. Myndigheterna känner själva bäst sina ekonomiska och administrativa begränsningar och eventuella luckor i den tekniska mognaden.

Inte heller bör myndigheternas IT-användning utformas så att enskilda åläggs att kommunicera elektroniskt; övergången till IT bör även i detta avseende vara frivillig.

Den tekniska utvecklingen och hittillsvarande lagstiftningsarbete på IT-området har visat att en användning av signerade elektroniska handlingar och anknytande rutiner för kommunikation gör det möjligt att med bibehållen säkerhet datorisera också rutiner där det ställs höga krav på rättssäkerhet, integritetsskydd, informationssäkerhet m.m.[12] Det internationella standardiseringsarbetet pekar också i riktning mot en

[11] Visserligen bör handlingar som kommer in till en myndighet vara anpassade till mottagarens tekniska och administrativa förutsättningar, men sådana begränsningar bör kunna frångås dels för att undvika rättsförluster som kanske framstår som slumpartade, dels för att stödja en önskvärd utveckling på området.

[12] Som exempel kan nämnas ärendehandläggningen på tull- och skatteområdet.

fortsatt utveckling av digitala signaturer med anknytande tjänster för informationssäkerhet.

Vid utformningen av den nya regleringen på tull- och skatteområdet har lagstiftaren undvikit speciallösningar, till förmån för rutiner som är möjliga att inordna under gällande rättsliga principer. Regleringen har därför visat sig vara av intresse också för andra delar av förvaltningen.

Denna inriktning mot generellt tillämpbara rutiner blev möjlig genom att begreppet elektroniskt dokument infördes. Därmed kunde ett förfarande som i hög grad bygger på IT och telekommunikationer naturligt genomföras med endast smärre justeringar av författningsregleringen och utan att rubba de allmänna principerna.

Jag föreslår att man bygger vidare på dessa utgångspunkter med en användning av digitala signaturer, digitala dokument, osv. — utan avsteg från gällande rättsliga principer. Behovet av ett långsiktigt arbete för att från sådana utgångspunkter se över de olika regelsystem som berörs av datoriseringen är dock påtagligt. Med hänsyn till den snabba utvecklingen kan en sådan genomlysning emellertid inte avvaktas, och som redan framgått har jag enligt utredningens direktiv att lägga fram förslag av mer begränsad karaktär.

2.6 Vissa akuta behov av IT-anpassningar

De akuta behoven av IT-anpassning kan något förenklat sägas röra två olika nivåer av datorisering och två grupper av regler.

Den första nivån har samband med de nämnda planerna på att åtminstone någon på varje enhet i förvaltningen skall kunna nås med elektronisk post under år 1996.[13] Denna strävan kan antas leda till en utbredd användning av elektronisk kommunikation, där mottagna elektroniska handlingar skrivs ut och tillförs traditionella pappersbaserade akter, samtidigt som det IT-baserade materialet gallras.

Från mina utgångspunkter aktualiserar sådana rutiner en grupp av regler som skall gälla för alla myndigheter som kommunicerar elektroniskt med omvärlden. Det är främst frågor om inkommande handlingar och delgivning som tilldrar sig intresse: När har en elektronisk handling kommit in till myndigheten? Hur skall myndigheten förhålla sig till elektroniska handlingar som den av någon anledning inte kan överföra till läsbar form? Kan delgivning ske via elektronisk post?

Den andra gruppen av regler rör företrädesvis krav på att uppgifter skall lämnas i traditionella skriftliga handlingar och kanske även på att

[13] Elektronisk post och katalog i offentlig förvaltning — en förstudie initierad av Toppledarforum.

handlingar skall vara undertecknade. Dessa bestämmelser får naturligtvis sin största betydelse vid sådana genomdatorisera de rutiner som har införts inom bl.a. tullen och skatteförvaltningen, där IT-rutiner ersätter traditionella skriftliga handlingar och akter. Många myndigheter överväger nu huruvida det är möjligt att på liknande sätt gå över till elektronisk hantering av mål och ärenden.[14]

På dessa två ämnesområden lägger jag fram lagförslag.

2.7 Lagstiftningstekniken, m.m.

Det är uppenbart att den första gruppen av regler, som skall gälla för alla myndigheter som kommunicerar elektroniskt, enkelt måste kunna återfinnas av dem som hanterar myndighetens post, och att regleringen inte bör göras oförenlig med bestämmelserna för traditionell miljö. Såvitt gäller frågor om när en handling skall anses ha kommit in är en naturlig lösning att i rättegångsbalken (RB), FL och förvaltningsprocesslagen (1971:291; FPL) föra in nya regler, i direkt anknytning till nuvarande bestämmelser om inkommande handlingar.

Beträffande den andra gruppen av regler, dvs. regler som uppställer krav på att uppgifter skall lämnas i traditionella skriftliga handlingar, kunde det synas lämpligt att ändringar förs in i varje författning som berörs. Jag vill dock, åtminstone inte för närvarande, förorda en sådan lösning. Ett skäl är att den kräver en genomlysning av alla de regelsystem som kan komma att beröras — en genomgång som inte skulle kunna göras inom den tidsram som står till buds. Ett annat skäl är att behovet av IT-rutiner och möjligheten att införa sådana växer fram successivt på olika förvaltningsområden, och det är en fördel om en enhetlig, central reglering skapas som enkelt kan göras tillämplig där den behövs. Man måste också räkna med att en ny reglering av detta slag kan komma att behöva ändras eller kompletteras flera gånger under de första åren — bl.a. som en följd av andra pågående lagstiftningsprojekt — och då är det naturligtvis från praktisk synpunkt enklare med en central reglering.

Jag föreslår därför att de bestämmelser som behövs i lag för att krav på användning av traditionella handlingar skall kunna uppfyllas genom elektronisk kommunikation skall föras in i FL. Regleringen bör, med hänsyn till de snabba förändringarna på dataområdet, inte bindas till en viss teknik, utan baseras på den funktionalitet som, från rättsliga och

[14] Även för domstolarna övervägs om elektronisk hantering av uppgifter kan ersätta de skriftliga rutinerna; jfr Domstolsverkets rapport 1995:1 Domstolarnas registerföring med hjälp av automatisk databehandling, s. 32.

tekniska utgångspunkter, krävs i IT-miljön. Detta har betonats i tidigare lagstiftningsärenden, bl.a. med avseende på elektroniska dokument.[15]

Jag tar sålunda i det följande upp de områden där jag har funnit att det behövs lagändringar, nämligen

- bestämmelser om när en elektronisk handling skall anses ha kommit in till en myndighet (kap. 3).
- bestämmelser om delgivning med elektroniska handlingar (kap. 4), och
- en föreskrift som gör det möjligt att använda elektroniska handlingar trots att någon bestämmelse om förvaltningsförfarandet kräver användning av traditionella handlingar (kap. 5).

Innan jag går in på dessa lagstiftningsfrågor behandlar jag dock frågan om vilken terminologi som bör användas på området.

2.8 Vissa begrepp

När kommunikation som hittills skett muntligt eller på papper kan ske med användning av datorer och telenät behövs vissa begrepp som i principiella termer beskriver de nya meddelandeformerna; som tidigare framhållits bör dessa begrepp dock inte knytas till specifika tekniska lösningar.

Som det grundläggande begreppet föreslår jag *elektronisk handling*.[16] Detta begrepp bör definieras på sådant sätt att det inte kan täcka mer än begreppet upptagning i 2 kap. 3 § TF; orden "som kan läsas, avlyssnas eller på annat sätt uppfattas endast med tekniskt hjälpmedel" bör alltså ingå i definitionen.

Däremot ligger det naturligtvis en begränsning i förhållande till TF i att definitionen enbart skall gälla *elektroniska* handlingar.[17] Vidare avses endast sådana handlingar vars innehåll har bestämts av utställaren, dvs. inte s.k. potentiella upptagningar. En beskrivning av dessa sidor av begreppet elektronisk handling kan lämpligen hämtas från

[15] TDL-utredningen har uttalat bl.a. att det finns många tekniska metoder för att lagra data och för att åstadkomma en äkthetskontroll och att det varken är möjligt eller lämpligt att lägga en detaljerad teknisk beskrivning till grund för det rättsliga synsättet på de elektroniska dokumenten, samt att informationssystemen bör anpassas för att också nya säkerhetslösningar enkelt skall kunna införas (SOU 1989:20 s. 99).

[16] Ordet "elektronisk" har i IT-sammanhang kommit att användas som ett slags övergripande begrepp som kan rymma olika ADB-rutiner, t.ex. i uttrycken elektronisk post och elektronisk dokumenthantering. Härvid bör närvaron av elektroner dock inte anses vara avgörande för den juridiska begreppsbildningen. När data lagras på CD-skivor bränns i stället märken på ett underlag som kan läsas med laserteknik, och framtidens datorer kanske baseras på optisk teknik så att det rör sig om fotoner i stället för elektroner.

[17] Härmed avses uteslutas inte bara traditionella pappershandlingar utan också vanliga analoga bandinspelningar, dvs. information som inte representeras med bestämda symboler som kan kopieras utan kvalitetsförluster och t.ex. transformeras med kryptografiska algoritmer.

Datastraffrättsutredningens förslag till definition av elektroniskt dokument: "en bestämd mängd data".

Traditionella underskrifter kan produceras endast av fysiska personer. Det har dock blivit vanligt att handlingar som ställs ut av ett företag eller en myndighet utformas så att en viss logotyp eller ett liknande kännetecken får ersätta underskriftens funktion som äkthetstecken. På motsvarande sätt kan en IT-baserad "signatur" knytas till t.ex. ett företag eller en myndighet, utan omvägen via en ställföreträdare. Sådana rutiner aktualiseras bl.a. när handlingar framställs utan direkt mänsklig medverkan.

Jag föreslår att detta återspeglas i terminologin så att begreppet *digital signatur* får avse IT-baserade motsvarigheter till en underskrift av en fysisk person, medan sådana signaturer knutna till en juridisk person eller en myndighet betecknas *digital stämpel*. Dessa signaturer och stämplar bör definieras så att de skall göra det möjligt att kontrollera huruvida innehållet i handlingen härrör från den som framstår som utställare. Vidare bör det av definitionerna framgå att dessa rutiner baseras på en omvandling av en bestämd mängd data; jfr definitionen av elektronisk handling med definitionen av t.ex. digital signatur.

Jag föreslår alltså två begrepp med samma rättsliga funktion, en uppdelning som kan ifrågasättas från rent lagtekniska utgångspunkter. Utställaren av en vanlig urkund enligt 14 kap. 1 § andra stycket BrB behöver inte vara en viss fysisk person.[18] På både förvaltnings- och civilrättsområdena finns emellertid ett praktiskt behov av att kunna skilja mellan en individanknuten respektive en företags- eller myndighetsanknuten utställarangivelse. Till detta kommer att uttrycket signatur närmast leder tanken till något som en fysisk person har skrivit. För att få till stand en diskussion i denna del har jag stannat för att föreslå skilda definitioner av utställarangivelser knutna till individ respektive till företag och myndigheter.[19] För den händelse en enda definition som rymmer dessa fall bedöms som tillräcklig kan detta uppnås genom att stryka definitionen av digital stämpel samt orden "fysiska person" i definitionen av digital signatur.

I enlighet med hur begreppet dokument vanligtvis används när det gäller pappershandlingar, bör begreppet *digitalt dokument* här definieras som en elektronisk handling med digital signatur eller digital stämpel.

[18] Enligt lagmotiven skall utställaren vara i någon mån bestämbar, t.ex. såsom tillhörande en viss grupp av personer, exempelvis militärer på ett visst förband eller intagna på en viss anstalt.

[19] Såsom dessa definitioner har utformats inryms visserligen inte en utställarangivelse som varken är knuten till en individ, ett företag eller en myndighet. Det torde emellertid inte på de områden som här är aktuella finnas något praktiskt behov av ett begrepp som rymmer sådana sammanslutningar eller grupper av individer. Det är tillräckligt om ett till IT anpassat straffrättsligt skydd för digitala dokument rymmer sådana utställarangivelser.

Jag föreslår alltså legaldefinitioner av begreppen elektronisk handling, digitalt dokument, digital signatur och digital stämpel[20], och använder därvid begreppen "digital" och "dokument" i anknytning till säkra rutiner för handlingar med signaturer eller stämplar.

Av skäl som kommer att redovisas i kap. 5 föreslår jag att dessa definitioner tas in i förvaltningslagen.

Den föreslagna regleringen ger, med utgångspunkt från Datastraffrättsutredningens syn på dokument, skydd också för digitala dokument som en mottagare vidarebefordrar. Om den som mottar dokumentet kan vidarebefordra detta utan att utställarens digitala signatur går förlorad ger den ursprungliga signaturen ett skydd mot förvanskning även i detta led. När signaturen inte bevaras kan i stället mottagaren intyga (vidimera) eller mera formlöst ange att viss text härrör från angiven utställare och förse hela eller delar av den mottagna texten med sin digitala signatur. Vid en kontroll indikerar dessa rutiner, så snart en signerad eller stämplad handling har förvanskats, att handlingen inte (i sin helhet) härrör från angiven utställare, och detta fungerar oberoende av om förvanskningen är omfattande eller kanske har inverkat endast på något enstaka tecken i handlingen.

Det bör betonas att de begrepp jag har föreslagit inte är avsedda att påverka bedömningen av vad som är allmän handling enligt TF utan bara skall användas för att ange hur elektronisk ärendehandläggning får ske i olika sammanhang; det är alltså främst begreppen digitalt dokument och digital signatur/stämpel som är av praktisk betydelse.

Jag tar längre fram (avsnitt 6.1) upp de mer allmänna frågorna om tillämpningen av TF:s regler om allmänna handlingars offentlighet och sekretesslagens regler om diarieföring i anknytning till elektroniska handlingar som myndigheter har tillgång till via nät eller på liknande sätt.

[20] Jag har även övervägt att definiera elektronisk akt, i syfte att förenkla behandlingen av frågan om "akter" i IT-miljö och anknytande rutiner. Det visade sig emellertid att en sådan definition inte var nödvändig i lag för den reglering jag föreslår.

3 Inkommande handlingar

3.1 Gällande rätt — traditionella handlingar

I 10 § FL ges föreskrifter om när en handling anses ha kommit in till en myndighet. För domstolarna finns i huvudsak identiska regler i 44 § FPL och 33 kap. 3 § RB. I dessa paragrafer finns flera alternativa regler om när en handling skall anses ha kommit in.

(1) Enligt huvudregeln har en handling kommit in den dag[21] handlingen *fysiskt har anlänt* till myndigheten[22].

(2) Även om själva handlingen inte har anlänt anses den ha kommit in den dag en *avi* om en betald postförsändelse som innehåller handlingen fysiskt har anlänt till myndigheten. Motsvarande regler finns för telegram och liknande meddelanden.

(3) Som ett alternativ till att handlingen eller en avi har nått fram till myndigheten anges att handlingen eller avin *kommit en behörig tjänsteman tillhanda.*[23]

I paragraferna ges också två kompletterande bevisregler.

(4) Om det *kan antas* att handlingen eller en avi om denna *fysiskt har anlänt* till myndigheten en viss dag, anses den ha kommit in den dagen, om den kommit en behörig tjänsteman tillhanda närmast följande arbetsdag.

(5) Vidare anses en handling ha kommit in en viss dag, om det kan antas att handlingen eller avi om denna den dagen har *avskilts på postanstalt*[24] för myndigheten. Det är emellertid även här en förutsätt-

[21] Uttrycken "den dag" och "viss dag" avser hela det aktuella kalenderdygnet, dvs. till kl. 24.

[22] Normalt tas handlingen emot av någon som på myndighetens vägnar har att ombesörja detta men handlingen kan också, efter tjänstetidens slut, ha lagts i ett brevinkast genom vilket handlingen förpassas in i lokalerna eller placerats i en brevlåda som myndigheten satt upp i direkt anknytning till dessa (Hellners/Malmqvist, Nya Förvaltningslagen, 4 u., s. 105).

[23] Vem som är behörig tjänsteman i ett enskilt fall får bedömas med ledning av författning, arbetsordning, interna instruktioner etc., och platsen för mottagandet är inte avgörande. Det föreligger emellertid ingen skyldighet för en tjänsteman att ta emot en handling utom tjänsten, t.ex. under sin fritid i bostaden (Gullnäs m.fl., Rättegångsbalken I, s. 33:12 och Hellners/Malmqvist, a.a., s. 105).

[24] Avgörande är om handlingen har blivit insorterad i myndighetens postfack eller postbox (Hellners/Malmqvist, a.a., s. 109).

ning att handlingen kommer behörig tjänsteman tillhanda närmast följande arbetsdag.

3.2 Gällande rätt och tidigare utredningsförslag — elektroniska handlingar

FL skall enligt lagens förarbeten tillämpas även i fråga om ärendehandläggning som sker med hjälp av ADB, och fjärrskriftsmeddelanden räknas som "handling" i lagens mening.[25] På motsvarande sätt framgår att fjärrskriftsmeddelanden är att betrakta som handling enligt 33 kap. 3 § RB, och att sådana handlingar kan inkomma till rätten från telecentral eller, om domstolen har sådan utrustning, genom telex-, teletex- eller faxmeddelande.[26] Detsamma torde gälla för förvaltningsprocessen. I praxis har också vid flera tillfällen prövats hur bestämmelserna om inkommen handling bör tillämpas — inte om de är tillämpliga — vid användning av telefax.[27]

I samband med *tulldatoriseringen* aktualiserades frågan när ett elektroniskt dokument bör anses inkommet till en tullmyndighet i förvaltningsrättslig mening. Resultatet blev att det i tullagen togs in särskilda bestämmelser om inkommande elektroniska dokument, dels för att anpassa regleringen till de elektroniska handlingarnas karaktär och till begreppet "inkommen" enligt 2 kap. TF, dels som en anpassning till det förhållandet att meddelandena skall sändas till en särskild

[25] Bestämmelsen i 10 § FL överensstämmer i sak med 7 § 1971 års förvaltningslag (prop. 1985/86:80 s. 63). Av motiven till äldre lag framgår att fjärrskriftsmeddelanden är att räkna som handling i lagens mening, men att detta inte torde behöva anges uttryckligen (prop. 1971:30 s. 369; jfr s. 363 f.). I remissvar över Förvaltningsrättsutredningens betänkande Ny förvaltningslag (SOU 1983:73), ville några remissinstanser att det skulle klargöras när en ADB-upptagning skall anses ha kommit in (se Ds Ju 1985:6 s. 195 f.), men frågan berörs inte i regeringens proposition 1985/86:80 om ny förvaltningslag. Ett uttalande i samband med tulldatoriseringen — att FL:s regler om inkommande handling inte är utformade så att de täcker in elektroniskt dokument — bör inte leda till annan bedömning. Bestämmelsen, som numera finns i 13 § tullagen (1994:1550), och som oförändrad överförts från föregående tullag (1987:1065), avser en hårt särreglerad sektor, med speciella rutiner för den kommunikation som äger rum mellan näringslivet och en mottagningsfunktion, gemensam för hela landet (prop. 1989/90:40 s. 28, se dock Cecilia Magnusson Sjöberg, Rättsautomation, s. 322 f.).

[26] Prop. 1973:30 s. 80 och Gullnäs m.fl., Rättegångsbalken I, s. 33:11.

[27] Se bl.a. RÅ 1991 ref. 90 (jfr RÅ 1991 not 393) NJA 1991 C 29, 1993 s. 308, 1993 C 170 och 1993 C 194. — Kommunikation med användning av dagens telefaxteknik utgör endast ett segment inom området datorkommunikation. Skillnaden är marginell mellan överföringen av meddelanden enligt fax-standard respektive elektronisk post eller en vanlig filöverföring mellan datorer. Detsamma gäller för den ovan nämnda tekniken för teletex. Det direkta sambandet med IT fördunklas härvid av att rutinerna vanligtvis utformas så att förlagan för det meddelande som sänds finns på papper hos avsändaren och tas ut på papper hos mottagaren.

mottagningsfunktion, gemensam för hela riket. Ett elektroniskt dokument anses enligt dessa bestämmelser ha kommit in till en tullmyndighet när det blivit tillgängligt för myndigheten för överföring till sådan form att det kan läsas. Om avbrott skulle uppkomma mellan mottagningsfunktionen — dvs. den som på uppdrag av tullen förmedlar dokument — och en tullmyndighets informationssystem, skall ett elektroniskt dokument anses ha kommit in till myndigheten redan när det tagits emot och kan antas ha avskilts för myndigheten hos förmedlaren.[28]

Lagrådet anförde angående denna bestämmelse bl.a. att full överensstämmelse visserligen inte uppnås med TF:s föreskrifter om när en upptagning som avser personregister blir att betrakta som allmän handling, men att någon annan lösning, med hänsyn till syftet med bestämmelsen, f.n. ej synes vara praktiskt möjlig.[29]

Frågan om när ett elektroniskt meddelande skall anses inkommet har aktualiserats också på *skatteområdet*. I departementspromemorian Elektronisk dokumenthantering inom skatteförvaltningen (Ds 1994:80) har, i 4 kap. lagen (1990:325) om självdeklaration och kontrolluppgifter, följande bestämmelse föreslagits under rubriken "Inkommande upptagningar":

En upptagning anses komma in till en myndighet inom skatteförvaltningen

1. när upptagningen blir tillgänglig för myndigheten med ett tekniskt hjälpmedel som myndigheten själv utnyttjar för överföring i sådan form att den kan läsas, eller

2. när data som representerar upptagningen anländer till myndigheten och tekniskt hjälpmedel för överföring enligt 1 finns hos myndighet som skall förmedla upptagningen.

En upptagning anses vidare ha kommit in viss dag om det kan antas att data som representerar upptagningen har anlänt till myndigheten den dagen men inte kunnat

1. överföras enligt första stycket 1 eller 2 på grund av tekniskt fel i upptagningen, eller

[28] Se 13 § tullagen (1994:1550) samt prop. 1989/90:40 s. 4, 28 och 50, 1990/91:75 s. 3 och 39 och 1994/95:34 s. 8 och 129.

[29] TDL-utredningen uttalade i denna del bl.a. följande: De elektroniska dokumentens självständiga existens utgörs av möjligheten att få fram ett dokument i läsbar form och att kontrollera dess äkthet genom en ADB-teknisk kontrollprocedur. Var den fysiska bäraren av data som representerar informationen finns blir därför inte — såsom vid pappersdokument — avgörande. Enligt motiven till 10 § FL är det av vikt att samordna begreppen med tryckfrihetsförordningen. Det är därför naturligt att se ett elektroniskt dokument som inkommet i förvaltningslagens mening i samma skede som det enligt 2 kap. 6 § jämförd med 2 kap. 3 § TF anses vara inkommet. Om en myndighet har rätt att förfoga över lagringsenheten och därmed äger rätt att överföra den till läsbar form skall upptagningen därför anses inkommen även i förvaltningslagens mening. Att begreppet elektroniskt dokument — till skillnad från upptagningsbegreppet i tryckfrihetsförordningen — ges ett lås/staket, gör inte denna likformiga bedömning onaturlig (SOU 1989:20 s. 147).

2. tas emot på grund av fel i myndighetens mottagningsfunktion.

Beträffande handlingar i annan form finns föreskrifter i 10 § förvaltningslagen (1986:223).

Vid remissbehandlingen var flera remissinstanser kritiska eller tveksamma till förslaget att en handling skall anses inkommen i de fall då tekniska fel vidhäftar upptagningen, överföringen eller myndighetens mottagningsfunktion. Generaltullstyrelsen ansåg det angeläget att regleringen blir likartad den som tillämpas inom tullen. Utredningsförslaget har inte föranlett lagstiftning i den delen.

3.3 Överväganden

Frågan om när en handling är inkommen enligt FL, FPL respektive RB aktualiseras dagligen vid förvaltningsmyndigheter och domstolar, och nya rutiner utvecklas och införs på många områden. Av hänsyn till arbetets behöriga gång måste frågan om inkommande handlingar kunna avgöras enkelt och snabbt, oberoende av i vilken form och på vilket sätt en handling når en myndighet. Grunderna för bedömningen av om en elektronisk handling är att anse som inkommen bör därför vara enkla och uppfattas som naturliga, också av den som inte har ingående kunskaper på IT-området.

Det är därmed mindre lämpligt att, såsom vid tulldatoriseringen, utgå från när en myndighet har tekniska möjligheter att göra en handling tillgänglig i läsbar eller annars uppfattbar form. Å ena sidan kunde en sådan reglering leda till att en inlaga till en myndighet, som sänds till en allmänt tillgänglig elektronisk anslagstavla knuten till ett nät som myndigheten har teknisk åtkomst till, ses som en inkommen handling trots att myndigheten aldrig har använt anslagstavlan. Å andra sidan kunde en sådan reglering leda till att ett meddelande som verkligen har nått myndigheten, t.ex. via e-post, inte anses vara inkommet om myndighetens tekniska hjälpmedel för att överföra meddelandet till läsbar form är trasiga. En frist kan därmed löpa ut.

Undantag för att korrigera sådana oönskade resultat av en tillgänglighetsprincip tenderar att bli komplicerade, och en IT-anpassning av förfaranderegelerna rörande inkommande handlingar är så angelägen att man knappast kan avvakta den översyn av bl.a. TF:s regler om upptagningar som pågår i annan ordning. Jag föreslår i stället en nära anknytning till de regler som gäller i dag om när traditionella handlingar skall anses ha kommit in.

3.3.1 Överbringande av disketter och överföring via nät

Beträffande disketter eller andra databärare, som ges in med vanlig post eller lämnas t.ex. med bud i myndighetens lokaler, bör de ovan beskrivna reglerna om när vanliga handlingar skall anses inkomna kunna tillämpas oförändrade. En sådan lösning är lätt att förstå och torde inte kräva några författningsändringar, eftersom begreppet "handling" i 10 § FL, 44 § FPL och 33 kap. 3 § RB uppenbarligen innefattar även elektroniska handlingar på databärare. — Jag återkommer till frågan om vad som bör gälla när myndigheten inte kan omvandla data till läsbar form.

Beträffande kommunikation via nät är frågan mer komplicerad. Data frikopplas delvis från bäraren. Handläggaren är vanligtvis inte intresserad av om den elektroniska handlingen fysiskt lagras hos myndigheten eller på annan plats. Avgörande är i stället om han kan hantera data på ett rationellt sätt. Jag föreslår en utgångspunkt från vissa grundläggande moment hos de traditionella rutinerna.

Varje myndighet har en adress för den traditionella posthanteringen. Denna adress motsvaras vanligtvis av en postbox eller ett postfack där posten samlas, för vidare transport till myndighetens lokaler. I anknytning härtill finns rutiner för postöppning, diarieföring m.m. Enligt min mening bör varje myndighet som kommunicerar elektroniskt med omvärlden ha en eller flera elektroniska "postboxar", via vilka all elektronisk kommunikation med myndigheten i princip bör gå.

Den ordning och reda som kännetecknar traditionell adressering bör härvid eftersträvas också för elektronisk kommunikation. För att nå detta mål krävs insatser redan i nuvarande intensiva skede när nya tekniska och administrativa rutiner utvecklas på området. Bland annat är det viktigt att varje myndighet bestämmer vilken eller vilka av de olika elektroniska adresser som myndigheten förfogar över som skall vara myndighetens officiella adress(er), dit meddelanden till myndigheten som sådan skall adresseras. Dessa adresser bör sedan finnas på myndighetens brevpapper m.m. och anges i adresskataloger av olika slag. Jag behandlar dessa frågor vidare i *bilaga 5*.

Som huvudregel bör det alltså, för handläggningen av mål och ärenden enligt FL, FPL och RB, föreskrivas att en handling som översänds elektroniskt anses ha kommit in till myndigheten den dag då handlingen har anlänt till myndighetens elektroniska "postbox".[30] Denna regel avses motsvara huvudregeln för pappersbaserade handlingar och disketter m.m. Kravet på att bäraren av ett meddelande fysiskt skall ha

[30] Ett sätt att åstadkomma en ytterligare precisering av de föreslagna reglernas tillämpningsområde skulle kunna vara att göra dem tillämpliga bara vid kommunikation med den eller de elektroniska adresser som myndigheten i formell ordning hade bestämt och kungjort som sina officiella adresser. Jag har dock inte ansett det nödvändigt med en sådan precisering av förslagen.

anlänt till myndighetens lokaler ersätts således med ett krav på att data skall ha anlänt till myndighetens elektroniska "postbox". För att undvika termer som kan uppfattas som knutna ill en viss teknik — såsom t.ex. "elektronisk brevlåda" — föreslår jag att denna "postbox" beskrivs som myndighetens "elektroniska adress".[31]

3.3.2 Brevlådans fysiska placering är inte avgörande

Den reglering jag föreslår skiljer sig från vad som gäller i pappersmiljön, genom att det inte är avgörande var en elektronisk "postbox" för myndigheten fysiskt finns och till vilket informationssystem den är kopplad. Härigenom kan olika tekniska lösningar regleras på samma sätt.

En myndighet kan ha en sådan koppling till ett externt datanät att e-postmeddelanden m.m. befordras direkt till myndighetens informationssystem, utan att lagras[32] hos någon annan i avvaktan på att hämtas eller annars vidaretransporteras till myndigheten.[33] Därvid anses en elektronisk handling, i analogi med vad som gäller för traditionell post[34], ha kommit in när den har nått myndighetens elektroniska adress i myndighetens informationssystem.[35]

Myndigheten kan också ha en eller flera elektroniska motsvarigheter till en postbox hos ett befordringsföretag, via vilken e-post m.m. distribueras till myndighetens informationssystem.

Enligt huvudregeln för traditionell post är en handling inte inkommen förrän den har nått myndighetens lokaler.[36] Elektronisk post bör emellertid anses inkommen redan när data har nått en myndighets elektroniska adress hos den som förmedlar tjänsten, dvs. det elektroniska "utrymme"/den funktion hos befordringsföretaget där inkommande

[31] Jfr begreppet "teleadress" i 27 kap. 18 § RB (prop. 1994/95:227).

[32] Härvid avses inte sådan mellanlagring som kan äga rum under befordran, för att tjänsten för överföring av meddelanden fram till den elektroniska brevlådan skall fungera.

[33] En myndighet kan t.ex. ha en egen s.k. hemsida ("homepage") på Internet med anknytande funktioner för e-post m.m. Detta kan jämföras med den situation som skulle uppkomma om en myndighet kunde upprätta ett eget postkontor i sina lokaler. När en postsäck med traditionella brev nådde dit vore handlingarna att anse som inkomna enligt huvudregeln för inkommande handlingar.

[34] Det avgörande är inte tidpunkten för en handlings ankomst till en postanstalt utan tidpunkten för insorteringen i postboxen (prop. 1973:30 s. 80).

[35] Det kan inte uteslutas att en myndighets tekniska rutiner — när ett fel framträder — har utformats så att data visserligen kommit in i systemet men inte nått ända fram till "brevlådan". Sådana fel bör dock kunna förebyggas genom att denna risk särskilt beaktas när systemen konstrueras. De rättsfrågor som härvid framträder bör kunna lösas i praxis, med beaktande av behovet av skydd för en enskild som drabbas av ett fel i myndighetens system.

[36] En försändelse har dock — om sedvanliga rutiner följs — kommit in redan genom att den avskilts på postanstalt (om den kommer en behörig tjänsteman tillhanda närmast följande arbetsdag). Enligt huvudregeln inkommer emellertid handling genom att den av postens eller myndighetens personal bärs över till myndigheten.

elektroniska handlingar förvaras för myndigheten.[37] Annars skulle skyddet för den enskilde och bedömningarna i övrigt bli helt beroende av vilken teknisk och administrativ lösning för elektronisk kommunikation som en myndighet väljer. Detta skulle kunna leda till rättsosäkerhet och i sämsta fall rättsförluster för enskilda.

3.3.3 Kommit en behörig tjänsteman till handa

En skriftlig handling — eller en elektronisk handling på en databärare — anses som sagt vara inkommen när pappershandlingen respektive databäraren har överlämnats till en behörig tjänsteman i dennes bostad, vid en förrättning etc. På samma sätt bör en elektronisk handling som har överförts till en e-postadress som tjänstemannen innehar privat eller som arbetsgivaren tillhandahåller, utan att den utgör en officiell adress för myndigheten, anses inkommen när handlingen har kommit tjänstemannen till handa.

I IT-miljön aktualiseras emellertid vissa praktiska frågor. När någon lämnar en pappershandling eller en diskett till en tjänsteman, underrättas denne vanligtvis om vad handlingen rör, och tjänstemannen kan ställa kompletterande frågor. Detta är inte möjligt när handlingar överförs elektroniskt, och det bör ställas sådana krav för att handlingar skall anses ha kommit en tjänsteman "till handa" att opraktiska rutiner kan undvikas, där en elektronisk handling — t.ex. på en elektronisk anslagstavla eller en e-postadress där tjänstemannen sällan loggar in — skulle anses ha kommit tjänstemannen till handa, trots att det inte rimligen kan krävas att tjänstemannen känner till den översända handlingens existens. Ett annat exempel på praktiska hinder är när en tjänsteman via sin privata e-postadress prenumererar på s.k. distributionslistor eller annars får stora mängder elektronisk privat post. Han kan då sakna möjligheter att regelbundet gå igenom sin privata e-post; jfr att det i traditionell miljö inte ställs något krav på tjänstemän att regelbundet undersöka om post som delas ut i bostaden rör tjänsten, och att den som i ett mål eller ärende kommunicerar med en tjänsteman via hans privata adress får stå risken om tjänstemannen är bortrest eller inte öppnar sin post.[38]

Det bör alltså inte anses tillräckligt att tjänstemannen har fått veta att ett meddelande — vilket som helst — har nått hans privata elektro-

[37] Inkommandepunkten bör således inte senareläggas så att en handläggare måste ha kopplat upp sig eller annars överfört data från den elektroniska brevlådan hos en förmedlare till myndighetens informationssystem.

[38] En tjänsteman är inte heller skyldig att ta emot en handling utom tjänsten, t.ex. under sin fritid i bostaden.

niska adress.[39] För att den elektroniska handlingen skall anses inkommen i RB:s, FL:s och FPL:s mening bör han också ha fått klart för sig att fråga är om ett meddelande som rör tjänsten.[40] Jag föreslår att detta uttrycks så att handlingen skall ha "tagits emot av en behörig tjänsteman".

Nuvarande utveckling mot att elektronisk post ges in genom att sändas direkt till en handläggare i stället för till myndighetens adress bör alltså bromsas för att undvika rättsförluster för enskilda och det allmänna; jfr de komplikationer som en sådan utveckling skulle föra med sig t.ex. när en handläggare som ensam har tillgång till en e-postadress är bortrest.

3.3.4 Särskilt om telefax

Rättspraxis angående inkommande handlingar rör i de delar som nu är av intresse frågan om en handling har kommit in i rätt tid när den sänts för sent med vanlig post men påstås ha faxats inom fristen.[41] I flertalet fall har saken huvudsakligen gällt värderingen av den bevisning som åberopats till stöd för att ett telefaxmeddelande, som inte kunnat återfinnas av rätten, har kommit in viss dag. Bevisningen har härvid utgjorts av bl.a. sådana aktivitetsrapporter rörande avsända och mottagna telefaxmeddelanden som de flesta faxar och datorer med telefaxprogramvaror kan producera, samt av anteckningar i ombudens akter angående vidtagna åtgärder och kopior av de handlingar som påstås ha faxats.

De yttre faktorer som har tagits till utgångspunkt i praxis klargör sålunda inte närmare vid vilken punkt i överföringen som den elektroniska handlingen anses inkommen. Går denna gräns vid t.ex. telejacket hos mottagaren[42] eller vid myndighetens tekniska funktion för mottagande av telefaxmeddelanden?[43] Sådana gränsdragningar har knappast

[39] Att ett e-postmeddelande till en privat adress rör adressatens tjänst framgår vanligtvis först vid en läsning av själva meddelandet eller en ärendemening på en meny över inkommande e-post.

[40] Det är alltså inte tillräckligt att en tjänsteman har hämtat e-post till sin dator via t.ex. en uppringd förbindelse, eller att en viss ikon på hans hemdator har gjort honom uppmärksam på att han har fått e-post.

[41] Se bl.a. NJA 1991 C 29, 1993 C 170, 1993 C 194 och 1993 s. 308 samt RÅ 1991 ref. 90.

[42] Jfr de komplikationer som tidigare framträdde vid verkställighet av beslut om hemlig teleavlyssning, till följd av att avlyssningsutrustningen fick anslutas endast till det allmänt tillgängliga telenätet. Det var ofta tveksamt var gränsen till privata nät gick, se vidare prop. 1994/95:227.

[43] Begreppet handling i berörda bestämmelser bör inte förstås så att endast traditionella skriftliga handlingar innefattas och att mottagandet därmed skulle ske först genom utskriften. I motiven till FL uttalas att lagen är tillämplig också när datorer används vid ärendehandläggningen (prop. 1985/86:80 s. 57) och genom en ändring i 33 kap. 3 § RB har nyligen klargjorts att telefax kan godtas för sådana inlagor som inte behöver vara

fyllt någon praktisk funktion med nuvarande rutiner där använda faxar och anknytande administrativa rutiner begränsat underlaget för rättens prövning till vissa aktivitetsrapporter och manuella noteringar.[44]

Utvecklingen går emellertid mot att faxrutiner integreras i avancerade informationssystem så att inkommande telefaxmeddelanden lagras i elektroniska "postboxar", t.ex. på en hårddisk i avvaktan på utskrift eller omdirigering till elektroniska akter och arkiv.[45] En sådan IT-användning gör det möjligt att införa säkra rutiner för *loggning* där hela meddelanden samt uppgifter om teleadresser och tidpunkter m.m. registreras. Enligt min mening bör det kunna krävas att myndigheter, i vilkas verksamhet bevis- och gränsdragningsfrågor av dessa slag har praktisk betydelse, ser till att de tekniska hjälpmedlen registrerar de uppgifter som behövs för rättssäkra förfaranden vid kommunikation mellan enskilda och myndigheten och att uppgifterna administreras korrekt.

Därmed blir den precisering av inkommandepunkten som jag föreslår betydelsefull också för kommunikation via telefax; det avgörande blir när meddelandet når myndighetens tekniska funktion för mottagande av telefaxmeddelanden.

3.3.5 En hjälpregel för oklara fall?

Nya IT-rutiner, där loggar, kvittenser och andra kontrollåtgärder införs, ger som sagt helt nya möjligheter att säkra bevisning, bl.a. om när en handling har kommit till en viss teknisk funktion i ett nät eller nått en funktion för att ta emot och lagra meddelanden i ett visst informationssystem. Dessa säkerhetsrutiner grundas på kontroller av om data har nått en viss funktion (från rättslig utgångspunkt, en viss mottagare). Genom sådana mer utvecklade kontrollrutiner, samt säkra rutiner för hantering av trafikrapporter m.m. som produceras med användning av faxar, skapas underlag för att bedöma om och i så fall när data har nått fram. Tekniska missöden kan emellertid inträffa så att t.ex. loggar och kvittenser sätts ur spel, och den mänskliga faktorn som felkälla bör inte underskattas.

Tolkningsregeln i gällande rätt (andra stycket i 33 kap. 3 § RB, 44 § FPL och 10 § FL) är tillämplig endast om en handling, som kan antas ha anlänt till myndigheten eller ha avskilts för myndigheten viss dag, har kommit behörig tjänsteman till handa *närmast följande*

egenhändigt undertecknade (prop. 1993/94:190 s. 106 f. och 121).

[44] Med ett sådant underlag torde det endast i mycket speciella undantagsfall kunna bli av intresse om inkommandepunkten knyts till om data "passerat mottagarens telejack", elektroniskt nått hans faxutrustning eller skrivits ut.

[45] En vanlig tilläggsfunktion till elektronisk post torde vara att handläggaren med samma tekniska utrustning kan faxa meddelanden.

arbetsdag. En sådan regel passar bäst för traditionell postbefordran där brev nära nog undantagslöst når fram till mottagaren. I IT-miljön framträder andra risker, och när missöden inträffar i denna miljö är det vanligt att den elektroniska handlingen inte alls kommer fram. Det finns alltså risk att en tolkningsregel för elektroniska meddelanden efter förebild av gällande rätt bara undantagsvis blir tillämplig när överföringen har skett endast elektroniskt.

Enligt min mening bör emellertid tolkningsregeln ändå begränsas till sådana fall där handlingen kommer en behörig tjänsteman till handa dagen efter att fristen löpt ut. Utan en sådan begränsning skulle osäkerhet uppkomma om huruvida en viss frist har löpt ut, t.ex. vid utfärdande av lagakraftbevis.[46] Detta gäller särskilt som det i gällande rätt angivna beviskravet ("kan antas") i praxis har tillämpats tämligen liberalt.

Jag föreslår därför att behovet av skydd för den enskilde, såsom i gällande rätt, tillgodoses genom en bevisregel för de fall där handlingen nästa dag når en behörig tjänsteman. Utan någon sådan regel alls skulle för övrigt mina andra förslag leda till att skyddet försämrades för den som sista dagen inom en frist sänder ett elektroniskt meddelande, t.ex. per telefax, och nästa dag överbringar handlingen till en behörig tjänsteman.

I övrigt bör den enskilde skyddas främst genom högt ställda krav på myndigheternas tekniska och administrativa rutiner för att hantera sina elektroniska adresser. Vanligtvis kan avsändaren presentera en trafikrapport, en logg eller någon liknande notering som visar att en elektronisk handling har sänts iväg.[47] Ett bevis om att meddelandet har sänts iväg bör emellertid inte anses tillräckligt. Utgångspunkten bör alltjämt vara att handlingarna överförs på avsändarens risk. Om brister i de tekniska eller administrativa rutinerna medför att data inte når fram, har det inte kommit in någon handling.[48]

Finns det uppgifter hos myndigheten om mottagande av en handling viss dag, som motsvarar avsändarens uppgifter om avsändande, eller uppgifter om att myndighetens tekniska utrustning skulle ha varit ur funktion vid just det aktuella tillfället, så att meddelanden som *nått* myndighetens elektroniska adress förstörts eller annars kommit bort,

[46] Jfr prop. 1973:30 s. 81 och Hellners/Malmqvist, Nya förvaltningslagen, 4 u., s. 111 f.

[47] Det torde bli vanligt att hela meddelandet därvid loggas.

[48] Till följd av förslaget att, beträffande elektronisk post, behandla de situationer lika där ett meddelande nått en elektronisk brevlåda hos ett befordringsföretag eller en elektronisk brevlåda i myndighetens informationssystem, behövs ingen särskild bestämmelse för det fallet att ett meddelande har avskilts för myndigheten hos en befordrare.

ligger det naturligtvis närmare till hands att anta att meddelandet har kommit in den dagen.[49]

Samtidigt som myndigheterna bör vidta de åtgärder som behövs för att undvika osäkerhet om huruvida handlingar har nått myndighetens elektroniska adress, bör de enskilda uppmuntras att ta tillvara de nya metoder som tas i bruk för att visa att en handling inte bara har sänts iväg utan också har kommit fram. Som exempel kan nämnas standardiserade rutiner för e-post, där avsändaren kan beställa en kvittens på att meddelandet har nått mottagarens elektroniska adress. Om sådana kvittenser administreras så att riskerna för manipulationer är begränsade, får de vanligtvis anses ge tillräckligt underlag för att en kvitterad handling har kommit in den dag som anges på kvittensen.

I övrigt får det anses tillräckligt att felaktigheter vanligtvis kan korrigeras genom återställande av försutten tid.

3.3.6 Särskilt om telegram, m.m.

Enligt gällande rätt kan telegram och andra fjärrskriftsmeddelanden överbringas också *muntligt*, t.ex. via telefon, under förutsättning att det är ett telebefordringsföretag som underrättar adressaten om handlingen eller om handlingens innehåll.[50]

Enligt uppgifter från Telia AB avlämnas telegram till myndigheter vanligtvis genom att meddelandet telefoneras ut eller sänds via telefax eller telex. När meddelandet telefoneras ut, sänds det oftast också med post, medan meddelanden som befordras till myndigheten via telefax eller telex postas endast om myndigheten så önskar. Befordran med bud av annat än s.k. lyxtelegram förekommer inte.

Hela meddelandet — i stället för en underrättelse om meddelandet — kan numera befordras till myndigheten med telefax, eller kanske med telex eller e-post. Därmed blir själva handlingen att anse som inkommen enligt den regel jag föreslår för elektronisk överföring — en rutin som kan användas ända till kl. 24 den dag en frist löper ut. Regeln om fjärrskriftsmeddelanden förutsätter däremot att en behörig tjänsteman nås av en underrättelse. Det kan därmed ifrågasättas om bestämmelsen angående fjärrskriftsmeddelanden behövs (andra meningen i första stycket av 33 kap. 3 § RB, 10 § FL och 44 § FPL). När myndigheterna har telefax saknas det anledning att överbringa muntliga meddelanden per telefon, med de risker för missförstånd som föreligger när mottagaren skall nedteckna ett uppläst meddelande. För den som inte har

[49] Se vidare hur Högsta domstolen formulerade sin bedömning av beviskravet i NJA 1993 s. 308, där en handling som skulle ha kommit in senast den 20 mars 1991 kom in först den 4 april samma år.

[50] Se bestämmelserna i första stycket andra meningen av 33 kap. 3 § RB, 10 § FL och 44 § FPL.

tillgång till telefax eller telex tillhandahåller bl.a. Telia AB tjänster varigenom meddelanden kan ringas in för att vidarebefordras (s.k. fonofax och fonotelex).[51] Det är alltså bara i udda fall som särreglerna för telegram m.m. leder till en förmånligare bedömning för ingivaren än de regler jag föreslår. Det bör därför övervägas att ta bort särreglerna för telegram m.m. Jag lägger emellertid inte nu fram något sådant förslag eftersom mitt uppdrag är begränsat till sådana författningsändringar som behövs för en IT-anpassning av berörda regelverk.[52]

3.4 Tekniska och administrativa hinder mot att läsa inkomna data

En annan fråga är vad som bör gälla när myndigheten inte kan läsa eller annars ta del av data som *har* inkommit.[53] Såväl beträffande ingivna databärare som teleöverförda data kan komplikationer uppträda till följd av att mottagaren (för tillfället) saknar tekniska hjälpmedel eller de kunskaper som behövs för att överföra aktuella data till läsbar eller annars uppfattbar form. Det kan också vara så att avsändaren eller någon förmedlare har förfarit felaktigt eller använt utrustning som inte fungerat korrekt.

Jag föreslår en praktiskt inriktad lösning, dels för att undvika tekniskt komplicerade utgångspunkter för den rättsliga bedömningen, dels för att finna synsätt som — så långt det är möjligt — inte görs beroende av de snabba förändringarna på IT-området. Härvid framstår det som naturligt att knyta an till den reglering som gäller för handlingar på främmande språk eller i punktskrift (8 § FL, 50 § FPL och 33 kap. 9 § RB).

[51] Om ett telegram i något fall skulle komma från ett hörn av världen där endast kommunikation via telegram når Sverige tillräckligt snabbt, kan telegrammet enkelt vidarebefordras via telefax från det svenska telebefordringsföretaget till adressaten. Även Posten erbjuder tjänster varigenom t.ex. telefaxmeddelanden kan befordras.

[52] En annan föråldrad bestämmelse finns i KK (1947:643; i dess lydelse enligt SFS 1993:619) om överbringande av rättegångsfullmakt genom telegram. Bakgrunden är att en skriftlig fullmakt skall ges in i original (12 kap. 9 § RB). Skriftliga fullmakter får emellertid överbringas genom telegraf eller telefon enligt de närmare föreskrifter som ges av regeringen (12 kap. 10 § RB). I den nämnda kungörelsen om överbringande av rättegångsfullmakt genom telegram föreskrivs dock att fullmakten skall uppvisas i original hos telebefordringsföretaget. En kopia, översänd via t.ex. fax, är inte tillräcklig eftersom fullmakten kan återkallas genom att originalet återtas eller förstörs. Jag har från Telia inhämtat att det nu finns endast ett inlämningsställe för telegram — beläget i Stockholm — där avsändaren kan visa upp fullmakten.

[53] Detta får inte förväxlas med frågan om vilket formellt innehåll (jfr t.ex. 33 kap. 1 § RB) eller vilket materiellt innehåll (jfr t.ex. 42 kap. 2 och 7 §§, 45 kap. 4 § samt 50 kap. 4 och 9 §§ RB) en inlaga bör ha.

Som en allmän princip gäller att svenska språket skall användas i inlagor och andra inkommande handlingar.[54] De regler som år 1973 infördes i rättegångsbalken innebär att domstolen vid behov får låta översätta handlingar som kommer in till rätten. Samtidigt infördes en bestämmelse som gav domstolen möjlighet att förelägga den part från vilken en handling på främmande språk inkommit att tillhandahålla en bestyrkt översättning. Detta alternativ togs bort ur lagtexten år 1987, som en följd av att paragrafen anpassades till vad som gäller för förvaltningsmyndigheter och förvaltningsdomstolar. Ändringen innebär emellertid inte att det aldrig blir aktuellt att låta parten översätta handlingen. Vid domstolens prövning av om det finns behov av att genom rättens försorg ordna med en översättning, får också vägas in vilka möjligheter parten har att själv få fram en översättning.[55]

Innan en handling har översatts får den i regel anses vara så ofullständig att den inte kan tjäna till grund för rättegången. Konsekvensen av att domstolen i förekommande fall inte finner skäl att låta översätta en viss handling, och att parten inte heller ombesörjer en översättning, blir att handlingen lämnas utan avseende på samma sätt som en på svenska avfattad gravt ofullständig skrift.[56]

I analogi med detta system föreslår jag att det skall ses som en allmän princip att en elektronisk handling som sänds in till en myndighet skall ha sådant format m.m. att den enkelt kan hanteras med mottagarens tekniska hjälpmedel. Myndigheten bör emellertid vid behov ha rätt att tekniskt bearbeta handlingen så att den kan läsas och att anlita tekniskt biträde för sådana bearbetningar. Även t.ex. datorprogram eller inspelningar av ljud kan behöva konverteras för att användas vid myndigheten, bl.a. som bevismaterial. Jag föreslår därför att konvertering skall få ske även för att data annars skall kunna uppfattas (förslagen i 33 kap. 9 a § RB, 52 a § FPL och 8 § andra stycket FL).

Om myndigheten inte kan eller inte finner skäl att vidta eller låta vidta de åtgärder som krävs för att läsa eller annars ta del av en elektronisk handling, och ingivaren inte tillhandahåller handlingen så att myndigheten kan ta del av den, får inkomna data lämnas utan avseende på samma sätt som en gravt ofullständig skrift.

Myndigheten bör emellertid vara skyldig att vidta de åtgärder som kan anses rimliga i det enskilda fallet. Det är knappast möjligt att i detalj ange vilka åtgärder en myndighet härvid bör vidta. Utvecklingen är snabb och en närmare reglering torde snabbt komma i konflikt med nya rutiner. Till stor del bör dock de komplikationer som uppkommer kunna lösas genom informella kontakter med ingivare, där de nya

[54] Prop. 1973:30 s. 71.

[55] Prop. 1986/87:89 s. 170.

[56] NJA II 1973 s. 246 och Gullnäs m.fl., Rättegångsbalken, s. 33:20.

rutinerna för kommunikation — inklusive telefax — kan tas i bruk för att snabbt få de upplysningar m.m. som behövs för att ta del av inkommande elektroniska handlingar. En annan möjlighet är att anlita något dataserviceföretag eller att inrätta gemensamma stödfunktioner som kan betjäna större områden. Det är vidare sannolikt att standardiseringen av rutinerna och olika tjänster för informationssäkerhet på sikt leder till att de tekniska komplikationerna begränsas.

Varje myndighet bör på lämpligt sätt upplysa om vilka format etc. som myndigheten använder. Sådana upplysningar kan lämnas t.ex. på brevpapper eller i kataloger som upptar myndigheternas e-postadresser.

För att kunna utnyttja möjligheterna till rationaliseringar fullt ut bör myndigheterna också ges rätt att anlita tekniskt biträde för att konvertera elektroniska handlingar som expedieras från myndigheten.

Kostnaderna för teknisk bearbetning av handlingar som en myndighet låter utföra bör enligt min mening betraktas som hänförliga till själva förfarandet och därmed stanna på staten. Vid en jämförelse med regleringen beträffande tolk (33 kap. 9 § RB, 50 och 52 §§ FPL och 8 § FL), framgår att en sådan kostnadsregel har upptagits i RB och FPL men inte i FL. Jag föreslår på motsvarande sätt att regler om kostnader vid konvertering förs in i RB och FPL men inte i FL. Ett alternativ som bör övervägas är naturligtvis att föra in enhetliga regler om tolkning, översättning och konvertering samt om kostnaderna för sådana åtgärder i alla tre lagarna.

3.5 Bekräftelse av handlingar som saknar underskrift i original

Jag föreslår att bestämmelsen angående bekräftelse av ett meddelande som saknar avsändarens underskrift i original (tredje stycket i 33 kap. 3 § RB, 44 § FPL och 10 § FL) flyttas, eftersom bestämmelsen bör komma efter samtliga regler om inkommande handlingar (förslaget till 33 kap. 3 b § RB, 44 b § FPL och 10 b § FL). Därvid bör en anpassning av ordalydelsen i de skilda bestämmelserna ske.

De förtydliganden som år 1994 gjordes i 33 kap. 3 § tredje stycket första meningen RB bör föras in också i FPL och FL så att det klart anges att en bekräftelse kan begäras, inte bara i de fall där avsändarens underskrift saknas helt utan också i de fall där avsändarens underskrift i original saknas.[57]

Jag föreslår vidare att bestämmelsen i 33 kap. 3 § tredje stycket andra meningen RB (jfr förslaget till 3 b §) om att rätten får bortse från meddelandet om en bekräftelse har begärts men rätten inte fått någon,

[57] Prop. 1993/94:190 s. 109.

förs in även i FPL och FL (förslagen till 44 b § FPL och 10 b § FL). Detta torde inte innebära någon ändring i sak.[58] Möjligheten att begära bekräftelse bör naturligtvis tillgripas endast när det behövs, och inget hindrar att en myndighet som har tagit emot en elektronisk handling utan signatur, godtar en signerad elektronisk bekräftelse när det är lämpligt. Beträffande förslaget att föra in denna bestämmelse i FL skulle visserligen kunna invändas att FL på många punkter är mindre utförlig än förfaranderegleme för domstolarnas handläggning av mål och ärenden och att det beträffande förvaltningsförfarandet vore tillräckligt att i denna del kunna lösa sådana frågor genom analogier med reglerna i FPL. Enligt min mening är det dock av värde om den processuella regleringen ges en enhetlig utformning och den föreslagna regeln — att myndigheten "får" bortse från ett meddelande som inte bekräftas — bör ge tillräckligt utrymme för att tillämpa bestämmelsen på sätt som är förenliga med de stora skillnaderna mellan olika förvaltningsområden.

Om denna bedömning godtas bör motsvarande regler i 4 kap. 10 § taxeringslagen (1990:324), 87 § uppbördslagen (1953:272), 20 kap. 10 § fastighetstaxeringslagen (1979:1152), 54 § lagen (1984:668) om uppbörd av socialavgifter från arbetsgivare och 4 kap. 4 a § lagen (1984:151) om punktskatter och prisregleringsavgifter kunna utmönstras.[59]

[58] Prop. 1993/94:190 s. 121; jfr Hellners/Malmqvist, Nya Förvaltningslagen, 4 u., s. 113.

[59] Jfr 15 kap. 6 § mervärdesskattelagen (1994:200).

4 Elektronisk delgivning

4.1 Utgångspunkter

När enskilda ges tillfälle att elektroniskt sända in handlingar till en myndighet aktualiseras också frågan om handlingar bör få delges med användning av elektronisk post (e-post).[1] En utgångspunkt bör härvid vara att de krav som gäller i traditionell miljö från bl.a. rättssäkerhets- och integritetsskyddssynpunkt skall kunna upprätthållas också i IT-miljön. Tekniskt kan sådana krav tillgodoses med användning av digitala signaturer och anknytande s.k. säkerhetstjänster.[2]

Enligt en av Toppledarforum initierad förstudie, Elektronisk post och katalog i offentlig förvaltning, är det motiverat att skapa förutsättningar för ett allmänt bruk av sådana rutiner. Samtidigt är det emellertid — enligt förstudien — viktigt att myndigheterna kommer i gång med elektronisk post, och de brister som kan finnas i olika elektroniska rutiner sägs därför tills vidare få kompenseras med tydliga rekommendationer om vad som lämpar sig för överföring via elektronisk post.

Redan nu finns vissa erfarenheter vid domstolar och andra myndigheter av att expediera handlingar elektroniskt med användning av telefax. Så länge dessa rutiner begränsas till t.ex. förfrågningar angående förhandlingsdagar, uppskov och enklare kompletteringar är riskerna för rättsförluster och andra olägenheter begränsade, och det har visat sig att den nya tekniken i viss mån gör det möjligt för myndigheterna att utan ökade resurser förbättra sin service. I praktiken behövs emellertid de nya rutinerna också på områden där kraven på säkerhet ställs högt.

[1] Jfr avsnitt 3.4, där frågan om tekniskt biträde för att konvertera handlingar som expedieras berörs.

[2] Om sådana rutiner utformas rätt kan de — på motsvarande sätt som för inkommande elektroniska handlingar — rent av ge ett effektivare skydd mot oavsiktliga och avsiktliga fel än traditionella pappersbaserade rutiner.

4.2 Nuvarande reglering

4.2.1 Delgivning eller mer formlös kommunikation

I delgivningslagen (1970:428) regleras gemensamt för rättegång och förvaltningsförfarande hur man skall förfara när en handling bevisligen skall bringas till någons kännedom. Med delgivning menas att en handling överbringas på sådant sätt att avsändaren får bevis om eller — på grund av legala presumtioner — äger utgå från att handlingen verkligen har kommit adressaten till handa.[3]

Bestämmelser om när en myndighet är skyldig att iaktta föreskrifter i delgivningslagen, och när det är tillräckligt att använda mer formlösa förfaranden, ges emellertid i andra författningar, bl.a. i RB, FPL och FL. För vissa fall föreskrivs uttryckligen att delgivning skall ske,[4] i andra har myndigheten att pröva om det med hänsyn till syftet med en bestämmelse om underrättelse framgår att delgivning bör ske, eller om delgivning ändå är påkallad med hänsyn till omständigheterna.[5]

4.2.2 Formerna för delgivning

I 3 och 3 a §§ delgivningslagen (DelgL) beskrivs olika sätt att delge; ordinär delgivning, särskild postdelgivning, telefondelgivning, stämningsmannadelgivning, kungörelsedelgivning samt förenklad delgivning, som är en form av ordinär delgivning. Endast reglerna om ordinär delgivning (inkl. förenklad delgivning) är utformade så att de lämpar sig för en anpassning till elektroniska rutiner. Vid en bedömning av vilka krav som bör ställas på elektronisk delgivning, från bl.a. rättssäkerhets- och informationssäkerhetssynpunkt, är emellertid också bestämmelserna om telefondelgivning av intresse.

Ordinär delgivning (3 § första stycket och 3 a § DelgL) rymmer fyra delformer. Handlingen kan sändas i lösbrev med begäran om delgivningskvitto eller rekommenderat med mottagningsbevis. En tredje delform, överlämnande med bud, är inte av intresse i detta sammanhang. Den fjärde formen av ordinär delgivning, s.k. förenklad delgivning, innebär att den som är part eller som har liknande ställning i ett mål eller ett ärende, under vissa förutsättningar kan delges genom att myndigheten sänder handlingen med post till den sökte under hans senast kända adress och minst en dag senare skickar ett meddelande om att handlingen har sänts. Sådan delgivning får emellertid användas

[3] NJA II 1971 s. 5.

[4] Se t.ex. 14 kap. 13 §, 25 kap. 4 §, 27 kap. 9 §, 33 kap. 5 §, 42 kap. 5 §, 45 kap. 9 och 16 §§, 47 kap. 5 §, 50 kap. 8 §, 51 kap. 8 §, 52 kap. 7 § RB.

[5] Se t.ex. 33 kap. 2 § första stycket RB, 47 § FPL, 17 och 21 §§ FL och övergångsbestämmelserna till delgivningslagen (1970:428); jfr prop. 1990/91:11 s. 14 f.

endast om den sökte (på annat sätt) har delgivits upplysning om att förenklad delgivning kan komma att användas, eller om sådan upplysning har sänts till den som har inlett förfarandet vid myndigheten eller som har gett in en handling i målet eller ärendet och upplysningen lämnas i nära anslutning till att ansökan eller handlingen har kommit in till myndigheten. Stämningsansökningar eller andra handlingar genom vilka förfarandet vid myndigheten inleds får dock inte delges förenklat. Dessutom krävs att förenklad delgivning inte är olämplig med hänsyn till omständigheterna.

Telefondelgivning (3 § tredje stycket DelgL) innebär att delgivning sker genom att en företrädare för en myndighet läser upp innehållet i en handling för den sökte på telefon och därefter sänder handlingen med post. Inte heller denna delgivningsform får användas beträffande handlingar genom vilka förfarandet vid myndigheten inleds. En ytterligare begränsning är att telefondelgivning får användas endast när det är lämpligt för att delge kallelser, meddelanden och andra handlingar, som inte är omfattande eller annars av svårtillgängligt innehåll.

4.2.3 När skall delgivning anses ha skett?

I 19 § DelgL ges en samlad reglering av *när* delgivning skall anses ha skett i vissa fall. Enligt huvudregeln har delgivning skett genom att den som söks för delgivning själv *har mottagit* handlingen, oavsett på vilket sätt den har kommit honom till handa (första stycket första meningen).[6] Härutöver finns ett antal i lagen uppställda presumtionsregler, som innebär att delgivning i vissa fall *skall anses ha skett*. Som exempel kan nämnas att telefondelgivning anses ha skett när de åtgärder som föreskrivs för sådan delgivning har vidtagits. Vidare anses förenklad delgivning ha skett viss tid efter att föreskrivna åtgärder har vidtagits, om det inte med hänsyn till omständigheterna framstår som osannolikt att handlingen före den aktuella fristens utgång kommit fram till den söktes senast kända adress. Dessa presumtionsregler är såväl beträffande förutsättningar som rättsverkningar noggrant angivna i lagen.

Den bevisning som säkerställs genom delgivning avser alltså antingen att en handling *har mottagits* av den adressat som söks, t.ex. ett undertecknat kvitto, eller att det *har förfarits på visst sätt*, t.ex. att de formella kraven för telefondelgivning eller delgivning genom kungörelse är uppfyllda i ett visst fall.

Frågan huruvida den som söks för delgivning har mottagit handlingen är föremål för fri bevisprövning. Genom att den sökte själv, på mottagningsbeviset eller postkvittot bekräftar att han mottagit handlingen, får myndigheten en garanti för att handlingen har nått fram till

[6] Bestämmelsen återspeglar det grundläggande syftet med delgivningen, nämligen att bereda den sökte tillfälle att ta del av försändelsens innehåll (NJA II 1978 s. 481).

honom.[7] Det finns emellertid inget hinder mot att en myndighet, på annat sätt än enligt formföreskrifterna i delgivningslagen, skaffar bevisning om att delgivning har skett. Myndigheterna bör således med tillämpning av fri bevisprövning avgöra om t.ex. en bekräftelse per telefon i ett enskilt fall kan godtas som bevis om att handlingen har tagits emot av den sökte.[8] Samma princip gäller när en handling överlämnas av ett bud som utfärdar intyg om att delgivning har skett på visst sätt. Beträffande intyg av stämningsmän och vissa andra befattningshavare har emellertid, av praktiska skäl, föreskrivits att intyget utan särskild prövning skall godtas som fullt bevis om att delgivning har skett.

I andra fall krävs inte något egentligt bevis för att handlingen har kommit adressaten till handa. I stället skapas en presumtion för att delgivning har skett när det har förfarits enligt lagens regler. Detta gäller t.ex. för den form av ordinär delgivning som betecknas förenklad delgivning. Denna presumtion kan emellertid motbevisas. Delgivning skall nämligen, enligt 19 § tredje stycket DelgL, anses ha skett om det inte med hänsyn till omständigheterna framstår som osannolikt att handlingen kommit fram till den söktes senast kända adress inom en tvåveckorsperiod.[9] Vid införandet av denna bestämmelse uttalade departementschefen bl.a. att det inte framkommit att de rättsmedel som finns har visat sig otillräckliga för att tillgodose befogade ändringsyrkanden som någon har framställt med åberopande av bristande delgivning.[10] Denna bedömning har senare bekräftats, se Domstolsverkets rapport (1993:6) Förenklad delgivning m.m. — en utvärdering.

4.2.4 Begreppet handling[11]

Enligt 6 § DelgL, i dess ursprungliga lydelse, skulle en handling som används för delgivning överbringas antingen i huvudskrift — dvs. i original — eller i styrkt avskrift eller styrkt kopia, och delgivning ansågs enligt 19 § samma lag ha skett genom att den som söks för delgivning har mottagit handlingen i original eller i form av avskrift/

[7] NJA II 1978 s. 469, där departementschefen vidare har uttalat att delgivningskvittot utgör ett tillförlitligt bevis för att den sökte är delgiven de handlingar han har kvitterat.

[8] NJA II 1978 s. 469 f. Här avses inte telefondelgivning enligt 3 § tredje stycket DelgL, prop. 1990/91:11 s. 27.

[9] Det krävs alltså inte att den sökte faktiskt har fått handlingen i sin hand. Han står själv risken om han på grund av bortavaro inte tar del av den, eller om handlingen skulle förkomma efter att den har avlämnats i adressatens brevlåda, postbox, etc.

[10] Prop. 1990/91:11 s. 26. Genom att det inte har föreskrivits någon absolut presumtion för att delgivning har skett när vissa formella förutsättningar föreligger, kan man rätta till uppenbara felaktigheter med tillämpning av ordinära och extraordinära rättsmedel (NJA II 1978 s. 483).

[11] Här bortses från sådan delgivning som avses i 20 § DelgL.

kopia som är bestyrkt. För de fall där en kopia har framställts *vid en myndighet* slopades dock år 1991 kravet i 19 § på att kopior skall vara vidimerade för att kunna delges med laga verkan. Vidare föreskrevs uttryckligen i 6 § att en kopia som har framställts vid en myndighet inte behöver bestyrkas.[12]

I 22 § DelgL föreskrivs att lagens bestämmelser om delgivning av handling tillämpas även vid delgivning av annat än handling. Av lagmotiven framgår emellertid att bestämmelsen avser "föremål" såsom varuprover och modeller,[13] inte flyktiga elektroniska signaler som överförs via nät eller överbringas genom att en databärare transporteras, och regleringen har utformats så att det direkt eller indirekt framgår att bestämmelserna i delgivningslagen huvudsakligen tar sikte på traditionella handlingar som fysiskt överbringas till den som söks för delgivning.[14]

För att överbringa det meddelande som skall delges *till den som har att verkställa* delgivningen, finns sedan länge föreskrifter som innebär att meddelanden kan överföras genom telefon, telegram eller på annat liknande sätt, 4 § DelgL och 10 § delgivningsförordningen (1979:101). Av 10 § delgivningsförordningen framgår bl.a. att en stämningsman, om en överföring sker via telefon, har att producera en handling och på den ange att den utgör ett riktigt återgivande av det telefonmeddelande han har mottagit.

4.3 Överväganden

4.3.1 Delgivning och kvittering med signerade handlingar

När sådana säkra rutiner för elektronisk dokumenthantering som beskrivs i bilaga 2 föreligger, finns det inte några sakliga skäl att delgivning inte skulle kunna ske elektroniskt. En elektronisk handling försedd med en handläggares digitala signatur eller myndighetens digitala stämpel översänds till den söktes elektroniska adress. Den sökte kan verifiera uppgiften om utställare av handlingen och huruvida texten har manipulerats; jfr en av myndigheten underskriven eller vidimerad pappersurkund. Ett elektroniskt delgivningskvitto bifogas med en begäran om att den sökte skall signera och återsända kvittot. Mottagaren kan — om han har tillgång till de tekniska och administrativa

[12] Enligt motiven tar regleringen sikte på alla slags kopior, t.ex. fotokopior, genomslagskopior, telefaxkopior och avskrifter (prop. 1990/91:11 s. 44 f.).

[13] NJA II 1971 s. 51. Jfr distinktionen i RB mellan skriftliga bevis och s.k. syneobjekt som är av intresse till följd av någon yttre egenskap, inte på grund av att de genom text eller på liknande sätt förmedlar ett visst föreställningsinnehåll.

[14] Telefondelgivning och kungörelsedelgivning kan nämnas som undantag.

hjälpmedel som behövs — genom några "knapptryckningar" signera och återsända t.ex. ett elektroniskt formulär för delgivningskvitto, om myndigheten har upprättat och bifogat ett sådant, eller helt enkelt returnera (ett exemplar av) den översända handlingen, efter att ha signerat den. Sådana rutiner torde, rätt utformade, ge i vart fall samma säkerhet som motsvarande traditionella rutiner.

Digitala signaturer och stämplar har emellertid inte ännu införts i sådan omfattning att delgivning och kvittering med signerade eller stämplade elektroniska handlingar (digitala dokument) kan antas bli vanlig under de närmaste åren.

4.3.2 Delgivning utan digitala signaturer eller stämplar

Utgångspunkten är att delgivning, i rättsligt reglerade former, skall ge rimliga garantier för att en viss handling, eller innehållet däri, når sin adressat. För myndigheterna blir det — i vart fall under den övergångsperiod då en utbyggd hantering av digitala signaturer och andra liknande tjänster för informationssäkerhet saknas — en viktig fråga om e-post och liknande rutiner kan användas för delgivning, trots att rutinerna inte når upp till de krav på säkerhet m.m. som anses gälla vid en användning av undertecknade pappershandlingar.

De principiella avvägningar som härvid aktualiseras, mellan å ena sidan intresset av effektiv delgivning och å andra sidan rättssäkerhets- och integritetsintressen, har belysts när delgivningslagen setts över i syfte att effektivisera delgivningsverksamheten.[15] Reformarbetet har inriktats på att bl.a. söka minska antalet delgivningar, att göra de existerande delgivningsformerna mer effektiva och att hitta nya delgivningsformer. Det har vidare övervägts huruvida kraven på bevisning för att delgivning har skett kan sänkas. Avsteg från kravet på bevisning måste emellertid vägas mot rättssäkerhetssynpunkter. Lagstiftaren har därför iakttagit viss försiktighet med delgivningsformer som innebär att någon fingeras eller presumeras ha fått del av en handling.

Enligt min mening bör det inte godtas att enskildas eller det allmännas rätt av effektivitetsskäl äventyras genom en reglering där risker för misstag och manipulationer blir påtagliga. Samtidigt måste lagstiftaren även i IT-miljön tillgodose parters och det allmännas befogade intresse av att kunna ta tillvara sin rätt eller annars vidta författningsenliga åtgärder gentemot den som tycker sig ha ett intresse av att förhala eller uppskjuta ett rättsligt förfarande.

De principiella ställningstagandena i samband med författningsändringar som har genomförts för att förenkla och effektivisera

[15] Jfr t.ex. prop. 1978/79:11, 1984/85:109 och 1990/91:11.

delgivning av traditionella handlingar, bör kunna tas till utgångspunkt också vid bedömningen av frågor om elektronisk delgivning.

4.3.3 E-post som ersättning för vanlig postdelgivning

Delgivning genom vanligt brev med begäran om delgivningskvitto är för närvarande det förfarande som bäst uppfyller de krav som bör ställas på ett billigt, snabbt, diskret och effektivt delgivningsförfarande.[16] Härvid har — i enlighet med principen om fri bevisprövning — inte krävts någon lagreglering av vilket bevisvärde ett undertecknat mottagningsbevis/delgivningskvitto skall anses ha.

Delgivning med e-post och liknande rutiner för elektronisk kommunikation skulle kunna bli ett synnerligen billigt och snabbt komplement, där den enskildes arbetsinsats skulle kunna begränsas till några "knapptryckningar". Det bör därför övervägas om ordinär delgivning med traditionell post kan ges en elektronisk motsvarighet, även om digitala signaturer eller motsvarande säkerhetsrutiner saknas. Härvid ger de överväganden som legat till grund för införandet av delgivningsformer som kompletterar ordinär delgivning via post viss vägledning — särskilt de avvägningar mellan effektivitet respektive skyddet för den enskilde som lades till grund för bestämmelserna om telefondelgivning och förenklad delgivning.[17]

När det saknas rutiner för elektronisk *"underskrift"* är det inte möjligt att inom ramen för den elektroniska handlingen verifiera huruvida texten omanipulerat härrör från den som framstår som utställare. Vid en jämförelse med traditionella handlingar kan konstateras att en namnteckning äkthet och manipulationer av den skrivna texten visserligen kan kontrolleras, t.ex. genom en kriminalteknisk analys. Sådana kontroller genomförs emellertid endast i de sällsynta undantagsfall där en handlings äkthet ifrågasätts. Underskriften fyller ändå sin funktion eftersom myndigheter och enskilda har tilltro till undertecknade urkunder. Lagstiftaren har vidare berett straffrättsligt skydd för denna tilltro.[18]

Någon motsvarande allmän tilltro torde knappast finnas för nuvarande allmänt spridda rutiner för elektronisk kommunikation. Såvitt gäller den handling som skall delges den sökte måste frågan emellertid ses i ljuset av att kraven på vidimering numera har upphävts beträffande traditionella kopior som har framställts vid en myndighet (6 § DelgL).[19] Visserligen kan det ifrågasättas om elektroniskt befordrade

[16] NJA II 1978 s. 469.

[17] NJA II 1985 s. 132 f. och prop. 1990/91:11 s. 16 f.

[18] Se 14 kap. 1 och 9 §§ BrB, jfr 15 kap. 12 § BrB.

[19] Prop. 1990/91:11 s. 43 f. och 50.

handlingar skyddas av bestämmelserna i 14 kap. BrB, eller ens av 15 kap. 12 § BrB om straff för den som sanningslöst utgiver handling, som tillkommit medelst genomslag eller fotografering eller på annat dylikt sätt, för riktig kopia av viss urkund.[20] Detta bör dock inte anses tillräckligt för att hindra elektroniska rutiner, och myndigheterna måste självklart logga eller annars förvara expedierade handlingar så att myndigheten, om någon ifrågasätter en handlings äkthet, kan visa vilket innehåll den hade när den avsändes; jfr kraven på utlämnande av allmänna handlingar och aktbildning m.m.[21]

Såvitt gäller delgivningskvitton i form av elektroniska handlingar utan digitala signaturer eller stämplar, måste den osäkerhet som dessa kan vara förenade med ställas mot de begränsningar av kraven på identifiering av den sökte som i traditionell miljö anses gälla för vissa fall. När bestämmelser om telefondelgivning infördes år 1985 förklarade departementschefen att den handläggande tjänstemannen bör inleda telefonsamtalet med att göra klart för sig att han samtalar med rätt person, en kontroll som bör ske genom att tjänstemannen frågar efter den söktes namn. Om det är den sökte som har ringt upp myndigheten eller det annars finns särskild anledning, bör tjänstemannen dock fråga även efter personnummer eller "annan uppgift som kan användas för en säker identifiering av den sökte". För den händelse osäkerhet ändå kvarstår beträffande identiteten bör telefondelgivning inte användas, fortsatte departementschefen.[22] När kretsen av handlingar beträffande vilka telefondelgivning får ske utvidgades år 1991, uttalades i lagmotiven att denna delgivningsform tillgodoser högt ställda krav på rättssäkerhet.[23]

Enligt min bedömning ger muntliga kontakter som tas per telefon knappast en högre säkerhet än e-post till och från elektroniska "postboxar" där skydd mot obehörig användning ges genom lösenord. Enskilda som mottar telefonsamtal som syftar till delgivning kan ge sig ut för att vara den sökte, medan det inte kan antas vara vanligt att den söktes e-postadress är tillgänglig för andra så att de falskeligen kan besvara elektroniska delgivningsförsändelser.[24] Det framstår inte heller

[20] Bestämmelserna i 14 kap. BrB om förfalskning av urkunder omfattar endast handlingar som har originalkvalitet. Elektroniskt befordrade handlingar utgör inte originalexemplar, utan "kopieras" via nät till adressaten.

[21] Myndigheten bör överväga att säkra inkomna och expedierade data genom elektronisk stämpel eller signatur. I vart fall bör loggar och "arkivexemplar" av elektroniska handlingar och akter förvaras säkert och skyddas mot manipulationer. Det är vidare självklart att de tekniska rutinerna för t.ex. uppdatering av vissa handlingar inte får sättas i funktion så att inkomna eller upprättade handlingar förändras.

[22] NJA II 1985 s. 132.

[23] Prop. 1990/91:11 s. 27.

[24] Motsvarande skydd ges inte för meddelanden till vanliga telefaxapparater. Det förekommer visserligen olika administrativa eller tekniska rutiner för att telefaxmeddelanden inte skall kunna läsas hos mottagaren av andra än adressaten, men

som sannolikt att en hacker eller en nätadministratör olovligen skulle ta del av en försändelse och dessutom falskeligen upprätta ett elektroniskt delgivningskvitto i den söktes namn. På motsvarande sätt är det svårt att se varför det skulle anses mera sannolikt att den sökte har nåtts av en telefondelgivning än av en handling vars mottagande har bekräftats per telefax, kanske med mottagarens telefaxkopierade logotyp och underskrift. Nuvarande ståndpunkt torde i stället bottna i att muntlig kommunikation via telefon — till skillnad från telefax- och e-postmeddelanden — har blivit så etablerad att kommunikationssättet med tiden kommit att åtnjuta tilltro.

Men naturligtvis måste de risker för manipulationer och misstag som framträder när elektroniska delgivningskvitton inte är signerade ändå beaktas. Jag föreslår den inskränkningen att elektronisk delgivning inte får avse stämningsansökningar och andra handlingar genom vilka förfarandet vid myndigheten inleds. I princip borde visserligen elektroniska delgivningskvitton *med* digital signatur kunna godtas, även med avseende på stämningsansökningar och liknande handlingar. Detta är emellertid inte för närvarande något praktiskt fall, och det är inte lagtekniskt okomplicerat att tillskapa en sådan ordning.

En utvidgning av den föreslagna begränsningen till andra handlingar vilkas innehåll är av ingripande natur för den enskilde är visserligen tänkbar, men en sådan gräns är inte heller enkel att dra och den skulle dessutom riskera att radikalt minska användningsområdet för elektronisk delgivning.[25] I stället föreslår jag den begränsningen att elektronisk delgivning får användas endast *när det är lämpligt*. I ett inledande skede torde sådan delgivning därmed i första hand komma att användas för brådskande kallelser och andra enklare meddelanden, såsom föreläggande som inte är av ingripande natur för den enskilde.[26]

Vid elektronisk delgivning uppkommer emellertid inte sådana risker för missförstånd som vid muntlig kommunikation via t.ex. telefon. I stället framträder risker för fel eller manipulationer vid överföringen och omvandlingen till läsbar form. I takt med att rutinerna för elektronisk kommunikation av handlingar blir säkrare och att myndigheterna får praktiska erfarenheter av tillförlitligheten hos olika rutiner för e-post m.m., bör mer betydelsefulla handlingar kunna delges genom elektronisk överföring.[27] Jag föreslår därför inga andra begränsningar av *vilka handlingar* som får delges genom elektronisk delgivning, än de som föreskrivs i gällande rätt för förenklad delgivning samt följer

avsändaren vet vanligtvis inte om sådana åtgärder har vidtagits hos en viss adressat.

[25] Jfr prop. 1990/91:11 s. 21 ang. motsvarande frågor vid förenklad delgivning.

[26] Jfr begränsningen av telefondelgivning till kallelser, meddelanden och andra handlingar som inte är omfattande eller annars av svårtillgängligt innehåll.

[27] Jfr 1991 års utvidgning av tillämpningsområdet för telefondelgivning (prop. 1990/91:11).

av mitt förslag att elektronisk delgivning får användas endast när det är lämpligt.

Elektronisk kommunikation bör inte användas när en enskild motsätter sig eller annars avböjer sådana rutiner, t.ex. för att han saknar erfarenhet av e-post eller annars har svårigheter att tillgodogöra sig elektroniska handlingar. Erfarna användare av e-post och den som själv valt att sända e-post till en viss myndighet bör däremot vanligtvis få godta att myndigheten använder elektronisk kommunikation. Myndigheten bör emellertid, även i dessa fall, tillmötesgå direkta önskemål om delgivning på traditionellt sätt. Skulle omständigheterna i något fall vara sådana att invändningen mot sättet för kommunikationen kan antas vara präglad av en önskan att förhala eller annars motverka handläggningen av ett mål eller ett ärende, bör den sökte också — när bevis om delgivning föreligger — som en serviceåtgärd därefter kunna få handlingen översänd i vanligt brev.

Begränsningen av elektronisk delgivning till fall där rutinen är lämplig rymmer också andra inskränkningar. Bl.a. bör risken för att utomstående läser telefaxmeddelanden eller e-postmeddelanden med för adressaten besvärande innehåll beaktas. Om rätten vet eller har anledning att anta att någon annan än den formella innehavaren av en elektronisk adress är användare av denna bör alltså försändelser med besvärande innehåll översändas med vanlig post, såvida inte insynsskydd i form av kryptering eller liknande föreligger; jfr vanliga förslutna kuvert. Sekretessbelagt material bör naturligtvis inte heller sändas elektroniskt, utom i sådana fall där tillförlitliga tekniska och administrativa rutiner ger tillräckligt skydd mot insyn.[28]

Vid delgivningen bör myndigheten — på samma sätt som vid vanlig postdelgivning — begära bevis om att den sökte har tagit emot handlingen. Härvid bör en handling som myndigheten överför elektroniskt kunna kvitteras både på traditionellt sätt, dvs. genom en pappersbaserad undertecknad handling, och elektroniskt. Kvittenser bör därvid i princip kunna godtas även i form av elektroniska handlingar utan signatur. Risken för manipulerade svar bör beaktas inom ramen för den prövning jag föreslår skall ske om elektronisk delgivning kan anses lämplig, varvid det bl.a. får betydelse hur viktig delgivningen är i det enskilda fallet.

Elektroniska meddelanden torde för övrigt redan i dag kunna användas som bevis om vanlig postdelgivning enligt 3 § första stycket; jfr 19 § första stycket DelgL. Jag föreslår inte några avsteg från principen om fri bevisprövning.

[28] Frågan om det är lämpligt att delge elektroniskt aktualiseras också om handlingen i något fall skulle vara att bedöma som personregister.

4.3.4 Förenklad elektronisk delgivning

Frågan om förenklad delgivning bör få ske i IT-miljön aktualiserar andra komplikationer. Det saknas ofta rutiner för kvittenser[29] samt för regelbunden "tömning" av elektroniska "brevlådor" och för distribution av telefaxmeddelanden från telefaxen till adressaten. Vidare aktualiseras risker för att fel e-postadress anges eller att försändelser annars kommer på avvägar under distributionen, se även *bilaga 5* om elektronisk adressering.

Enligt min mening får kommunikation via nät, utan en (automatisk) kvittens på att handlingen har nått den söktes elektroniska adress, anses vara förenad med sådana risker att förenklad delgivning genom elektronisk överföring inte bör komma i fråga. När mer utvecklade rutiner för elektronisk kommunikation föreligger bör dock delgivning baserad på en presumtion att en elektronisk handling har nått den sökte kunna aktualiseras. Ledning kan härvid hämtas från de överväganden som låg till grund för regleringen av (vanlig) förenklad delgivning.[30] Vid sådan delgivning anses den som har underrättats om att förenklade rutiner kan komma att användas, ha delgivits viss tid efter att meddelandet har sänts i vanligt brev till den sökte.

För att korrigera oönskade effekter anses förenklad delgivning dock ha skett endast om det inte med hänsyn till omständigheterna framstår som osannolikt att handlingen inom viss tid har kommit fram till den söktes senast kända adress. Omständigheter som kan medföra att förenklad delgivning inte har skett är enligt lagmotiven bl.a. att ena eller båda försändelserna kommer i retur eller att den sökte, t.ex. som en reaktion på meddelandet om den översända handlingen, anmäler att delgivningsförsändelsen inte har kommit fram.[31]

Risken för att meddelanden sänds till fel adress bör — när den som söks själv har sänt e-post till myndigheten — i viss mån kunna undvikas genom att myndigheten kopierar den adress den sökte angivit. Som jag återkommer till skall myndigheten, vid delgivning av en underrättelse att en förenklad form för delgivning via e-post kan komma att brukas, ange den e-postadress som myndigheten avser att använda. Denna adressangivelse bör också kunna kopieras för att undvika att fel adress anges när ett e-postmeddelande sänds.[32] Risken för fel i posthanteringen har beträffande traditionella brev, när två försändelser sänds vid olika tillfällen, bedömts som i det närmaste

[29] Dvs. besked om att e-post t.ex. har sänts, nått visst adress eller "öppnats".

[30] Prop. 1990/91:11 s. 17 f.

[31] Prop. 1990/91:11 s. 20. Vid kungörelsedelgivning torde större risker föreligga för att meddelandet inte når den sökte.

[32] Det bör vidare övervägas om rutinerna för e-post kan utformas så att en motsvarighet skapas till postens rutin att återställa traditionella brev med felaktig adress till avsändaren, t.ex. med noteringen "Adressaten okänd på angiven adress".

försumbar.[33] System för e-post där avsändaren får en automatisk kvittens — inte från mottagaren utan som en följd av automatiska kontrollrutiner — torde ge åtminstone samma grad av säkerhet, eftersom bedömningen baseras på ett positivt besked att meddelandet har nått fram till adressatens elektroniska adress, inte på en slutsats att meddelandet i avsaknad på andra indikationer kan antas ha nått adressaten.

Det framträder också andra risker för att den sökte inte får del av en handling som överförs elektroniskt. Någon kan obehörigen stoppa försändelsen, och kanske se till att kvittenser ändå genereras. Att *två* elektroniska försändelser som befordras olika dagar skulle komma bort, samtidigt som kvittenser genereras på att handlingarna har nått fram, framstår emellertid som osannolikt. Det kan vidare vara så att den som söks för delgivning är bortrest, en risk som vid förenklad delgivning har mötts genom att en handling inte anses ha kommit adressaten till del förrän viss tid efter det att försändelsen och underrättelsen har skickats med posten. I IT-miljön tillkommer helt nya möjligheter för adressaten att med tekniska hjälpmedel hämta sin e-post oberoende av var han befinner sig.

Enligt min mening bör alltså förenklad delgivning kunna komma i fråga även i IT-miljön, om pålitliga tekniska rutiner föreligger varigenom myndigheten får kvittens på att försändelserna har nått den aktuella elektroniska adressen.[34] Såsom för (vanlig) förenklad delgivning bör det föreskrivas att den sökte skall ha delgivits upplysning om att förenklad elektronisk delgivning kan komma att ske. Självklart måste det i denna underrättelse anges till vilken elektronisk adress en delgivningsförsändelse kommer att skickas; jfr *bilaga 5*. Därmed kan förenklad elektronisk delgivning ske endast efter en ny underrättelse om den sökte har bytt e-postadress.

Den som söks för delgivning bör emellertid — såsom vid traditionella förenklade rutiner — stå risken om han underlåter att ta del av den post som nått den angivna elektroniska adressen. Detsamma bör gälla för den i teorin tänkbara situationen att en handling skulle komma bort under transport, medan kvittenser ändå genereras.[35]

Förenklad elektronisk delgivning bör dock, som i traditionell miljö, inte få avse handlingar genom vilka förfarandet vid myndigheten inleds, och av rutinernas utformning följer att delgivning inte kan anses ha skett förrän viss tid förflutit från det att myndigheten fått kvittenser på att handlingen och meddelandet om handlingen har nått den söktes

[33] Prop. 1990/91:11 s. 19.

[34] Jfr mitt förslag till reglering av inkommande handlingar, där elektroniskt överförda handlingar anses inkomna redan när de har nått myndighetens elektroniska "postbox".

[35] Redan användningen av kvittenser torde ge en högre säkerhet än den presumtion som tillämpas vid förenklad delgivning med post.

elektroniska adress. Dessutom bör förenklad elektronisk delgivning få användas endast "när det är lämpligt". Härmed avses motsvarande begränsningar som i förslaget till reglering av ordinär elektronisk delgivning. Vidare bör förenklad elektronisk delgivning få ske bara med den som är part eller intar en liknande ställning; jfr 3 a § första stycket DelgL.

Mitt förslag, att förenklad elektronisk delgivning skall få användas endast när myndigheten får kvittenser på att handlingen och meddelandet om handlingen har nått den söktes elektroniska adress, medför att det inte behövs någon motsvarighet till regeln i 19 § DelgL om att (vanlig) förenklad delgivning anses ha skett endast när det inte med hänsyn till omständigheterna framstår som osannolikt att handlingen har kommit fram.

Däremot föreslår jag en bestämmelse som motsvarar 3 a § andra stycket andra meningen DelgL, enligt vilken en upplysning om att förenklad elektronisk delgivning kan komma att ske, inte behöver delges när vissa förutsättningar föreligger. Tillämpningsområdet för detta undantag har nyligen utvidgats så att det — utöver den som har inlett förfarandet vid myndigheten — också gäller den som har gett in en handling i målet eller ärendet.[36] Motsvarande bestämmelse för förenklad elektronisk delgivning bör ges samma tillämpningsområde. Naturligtvis får underrättelsen om att förenklad elektronisk delgivning kan komma att användas sändas endast med vanlig post, inte med e-post.

I samma lagstiftningsärende infördes vidare ett undantag från kravet att information om förenklad delgivning skall lämnas i varje instans.[37] Har svaranden under handläggningen hos kronofogdemyndigheten av ett mål om betalningsförelägganden eller handräckning delgetts upplysning om att förenklad delgivning, efter överlämnande, kan komma att användas i målet hos tingsrätten, Arbetsdomstolen eller Statens vanämnd, får svaranden delges sökandens begäran om överlämnande och andra handlingar i målet genom förenklad delgivning (3 a § tredje stycket DelgL).

Jag har inte funnit anledning att föreslå någon motsvarande undantagsbestämmelse för elektronisk delgivning (som i så fall måste göras tillämplig också på "vanlig" elektronisk delgivning). I vart fall för närvarande är det inte realistiskt att räkna med att myndigheterna i ett så tidigt skede av handläggningen av ett mål skall ha sådan kännedom om svarandens möjligheter att kommunicera elektronisk att en sådan bestämmelse skulle få någon praktisk betydelse.

[36] Prop. 1994/95:188 s. 16 f.

[37] A. prop. s. 12 f.

4.3.5 En definition av elektronisk handling, m.m.

Som framgått ovan är det tveksamt om elektroniska handlingar kan anses innefattade i delgivningslagens handlingsbegrepp. Jag föreslår därför att definitioner av elektronisk handling, digital signatur och digital stämpel förs in i delgivningslagen genom en hänvisning till de definitioner jag föreslår i FL (1 a § DelgL och 1 a § FL).

Undantaget i 6 § DelgL från kravet att kopior[38] som överbringas till den sökte skall vara bestyrkta bör härvid inte okritiskt överföras till den elektroniska miljön. Tanken med detta undantag har uppenbarligen inte varit att myndigheterna skall översända föreläggande och liknande handlingar i form av ovidimerade kopior, utan att befria från den betungande uppgiften att vidimera omfattande bilagor såsom stämningsansökningar med tillhörande handlingar, omfattande utredningar, etc. Den som söks för delgivning har alltså vanligtvis fått åtminstone en skrivelse från myndigheten i original, och när en stämningsman har överlämnat handlingar som han mottagit per telefax har i stället proceduren — stämningsmannens besök och begäran om underskrift på en blankett — visat att en myndighet ligger bakom.

Vid delgivning via e-post kan den enskilde på ett annat sätt ha fog för att ifrågasätta försändelsens ursprung. Visserligen kan den enskilde genom att kontakta myndigheten få bekräftat om de mottagna handlingarna härrör från angiven utställare, men de skäl som ligger till grund för att pappershandlingar inte bevittnas — den stora arbetsinsatsen — kan knappast åberopas om tekniska hjälpmedel finns för att med några "knapptryckningar" förse elektroniska handlingar med digitala signaturer eller digitala stämplar.[39]

Jag anser därför att en myndighet vid delgivning bör vara skyldig att förse sina elektroniska handlingar med digital signatur eller stämpel, när behövliga tekniska och administrativa rutiner finns hos myndigheten.[40] Under nuvarande skede där nya tillämpningar byggs upp är en närmare reglering i lag dock knappast möjlig. Jag föreslår därför endast den föreskriften att myndigheten skall förse elektroniska handlingar med digital signatur eller digital stämpel när det kan ske.

Visserligen kan de som söks för delgivning, i vart fall under en övergångsperiod, antas sakna tekniska hjälpmedel för att hos sig

[38] Handlingar kan i IT-miljön knappast sägas utgöra original*exemplar* eftersom tekniken bygger på ständigt mångfaldigande av vissa signalmönster — det finns endast ett original*innehåll.*

[39] Sådana tekniska kontrollrutiner gör det dock inte möjligt för mottagaren att hos sig verifiera ens myndighetens elektroniska skrivelse, när försändelsen överförs via olika tekniska miljöer där skydd baserade på kryptering inte bevaras intakta.

[40] Digitala signaturer och stämplar kan dessutom användas för att verifiera t.ex. att en viss handling har expedierats av en handläggare (signatur) eller för att verifiera att en annan åtgärd har vidtagits av någon som har tillgång till en myndighets eller en juridisk persons elektroniska stämpel.

verifiera myndighetens signatur eller stämpel. Utvecklingen går emellertid snabbt och det kan vara betydelsefullt för den sökte att ha möjlighet att överbringa mottagna handlingar till någon som kan verifiera dem, t.ex. till en advokat som har anskaffat sådana hjälpmedel.[41] Till detta kommer att bl.a. handlingsoffentligheten ger myndigheterna anledning att genom tekniska kontrollmetoder säkerställa vad myndigheten har sänt.

Det bör alltså inte krävas att en myndighet som överväger att delge elektroniskt kontrollerar huruvida mottagaren har tekniska hjälpmedel för verifiering och om de aktuella kommunikationslederna kan överföra de digitala dokumenten så att signaturen/stämpeln bevaras. Inte heller bör en myndighet som saknar rutiner för digital signatur eller stämpel hindras att använda elektroniska rutiner när det är lämpligt.

Som en anpassning till nyligen gjorda ändringar i delgivningslagen föreslår jag också en redaktionell ändring i 6 § tredje stycket DelgL.

[41] Detta kan jämföras med att traditionella underskrifter vanligtvis inte verifieras och att en säker verifiering kan kräva en analys av experter.

5 Elektroniska handlingar som ersättning för undertecknade handlingar m.m.

5.1 Vilka myndigheter berörs?

Den reglering jag föreslår i denna del avser bara myndigheternas ärendehandläggning. Som myndigheter anses regeringen, domstolarna och de statliga och kommunala förvaltningsmyndigheterna. Förfarandet vid de beslutande offentliga organen, såsom riksdagen och kommunfullmäktige, och vid de bolag och andra privaträttsliga subjekt som fullgör förvaltningsuppgifter, omfattas alltså inte av mina förslag. Vidare bör domstolarnas dömande verksamhet undantas. De rättsfrågor som aktualiseras vid en IT-anpassning av rättegångsbalken kan knappast lösas inom ramen för mitt begränsade uppdrag, och det pågår inte något arbete med att införa helt elektronisk dokumenthantering vid domstolarna. Visserligen överprövar domstolarna redan i dag ärenden som har dokumenterats elektroniskt, t.ex. av kronofogde- och skattemyndigheter, men dokumentationen skrivs då ut och sänds till domstolen på vanligt sätt.

Däremot bedriver en mängd förvaltningsmyndigheter projekt för att införa digitala dokument och elektroniska akter, så som på tull- och skatteområdet. I *bilaga 3 och 6* behandlar jag de frågor om arkivering och elektronisk akthantering som härvid aktualiseras.

För en begränsning av mina förslag till förvaltningsförfarandet talar också de stora skillnaderna mellan målhanteringen vid en domstol, i enlighet med RB:s och FPL:s detaljerade förfaranderegler, respektive handläggningen av förvaltningsärenden enligt FL, som är begränsad till basregler för sådana områden där rättsskyddssynpunkter spelar en dominerande roll.[1] I syfte att knyta an till FL:s tillämpningsområde utesluter jag dock inte domstolarnas handläggning av förvaltningsärenden.

Frågan om hur reglerna i FL bör tillämpas i IT-miljön behandlas också i *bilaga 7*, som rör frågor som inte tas upp i det följande.

[1] Prop. 1985/86:80 s. 11.

5.2 Vilka regelverk berörs?

De regelverk som aktualiseras på förvaltningsområdet kan i grova drag delas in i organisatoriska regler, kompetensregler, materiella regler och förfaranderegler. Mina förslag begränsas till reglerna om *förfarandet* vid förvaltningsmyndigheternas handläggning av ärenden och domstolarnas handläggning av förvaltningsärenden.

Under senare år har ett omfattande arbete bedrivits för att åstadkomma enhetliga sådana regler. Den nuvarande förvaltningslagen är ett resultat av detta arbete. Dessutom har ett stort antal specialförfattningar setts över i syfte att införa enhetliga rutiner. Trots dessa strävanden uppvisar emellertid den förvaltningsrättsliga regleringen en splittrad bild. Detta beror bl.a. på förvaltningsverksamhetens skiftande innehåll och regleringens uppdelning på olika lagar, som har tillkommit successivt för olika förvaltningsgrenar.

Det förvaltningsrättsliga författningsmaterialet är alltså synnerligen omfattande och uppdelat på en mängd författningar.[2] När elektronisk dokumenthantering införs behöver vissa av dessa regler anpassas till den nya miljön.

Det är knappast möjligt att inom ramen för mitt uppdrag göra en fullständig genomgång av alla förfaranderegler, som nu eller i en framtid kan komma att behöva IT-anpassas. Jag har därför utgått från FL och vissa andra författningar som är grundläggande för förvaltningsmyndigheternas handläggning av ärenden eller som kan ses som typfall vid en övergång till elektronisk dokumenthantering på myndighetsområdet.[3] Den följande genomgången syftar därför till att undersöka bl.a. om de anpassningar av förfarandereglerna, som behövs vid en övergång till säkra rutiner för elektronisk dokumenthantering, kan genomföras utan ändringar i varje författning som innehåller regler för traditionell dokumenthantering.

Härvid aktualiseras främst bestämmelser där fråga uppkommer om bestämmelsen skall anses innefatta ett krav på underskrifter eller annars på en användning av fysiska originalexemplar. Frågan uppkommer i anknytning till bl.a. begreppen "skriftlig" och "handling"[4], och krav i författningar på att handlingar skall vara "undertecknade" eller "egenhändigt undertecknade". Det är ett stort antal författningar på förvaltningsområdet som innehåller den berörda kategorin av begrepp och som reglerar förfarandet vid handläggningen av ärenden (jfr 3 § FL).

[2] Se vidare Strömberg, Allmän förvaltningsrätt, 17 u., s. 22.

[3] Jag har vidare sökt bilda mig en uppfattning på detaljnivå om rättsfrågornas omfattning och art genom att söka i Rättsdatasystemet med sådana nyckelord som erfarenhetsmässigt för med sig komplikationer i IT-miljön.

[4] Ang. handlingsbegreppet, se SOU 1992:110 s. 461 f. och den i rättspraxis behandlade frågan när ett telefaxmeddelande anses inkommet.

5.3 Vissa begrepp i FL

Jag har i avsnitt 2.8 föreslagit att det i FL skall föras in definitioner av elektronisk handling, digitalt dokument, digital signatur och digital stämpel. Frågan är om begreppsanvändningen i övrigt i FL hindrar sådan elektronisk dokumenthantering som jag förordar.

Vad först beträffar begreppet "handling" (se 10, 15, 25 och 27 §§ FL), framgår av motivuttalanden att regleringen av inkommande handlingar innefattar också fjärrskriftsmeddelanden.[5] Av lagmotiven framgår vidare att FL skall tillämpas också i fråga om ärendehandläggning som sker med hjälp av ADB.[6] Begreppet "handling" innefattar alltså även elektroniska handlingar.

Sådana uttryck som "anteckna" (15 och 19 §§), "det som har tillförts ärendet" (16 §), "skrivelse" (24, 25 och 30) och "skrivfel" (26 §), bör på motsvarande sätt förstås så att också IT-rutiner innefattas. Detsamma bör gälla för vissa underrättelser (17 § andra stycket och 21 § tredje stycket FL), som får ske (muntligt, genom vanligt brev, genom delgivning eller) "på något annat sätt".[7]

Utöver möjligheten att begära bekräftelse enligt 10 § tredje stycket FL uppställs inget krav på "underskrift". Som framgått ovan förordar jag att rätten att kräva bekräftelse i form av en i original undertecknad pappersurkund skall omfatta även elektroniska handlingar.

Slutligen aktualiseras frågan huruvida föreskrifterna om att underrättelse om beslut skall ske "skriftligt" om parten begär det (21 § FL), och att beslut överklagas "skriftligt" (23 § FL), skall anses innebära att elektroniska rutiner är uteslutna. Till att börja med utesluter kravet på skriftlighet naturligtvis muntliga rutiner. Vidare sägs ofta, både i Sverige och utomlands, att krav på "skriftlig"/"written" form i princip utesluter elektroniska handlingar. Närmare studier har emellertid visat att begreppet "skriftlig" i svenska författningar — när det ansetts lämpligt — har tolkats så att även elektroniska rutiner innefattas[8], och enligt Hellners/Malmqvists kommentar till FL måste det antas att lagens ordalag inte utesluter överklagande genom telegram eller annat

[5] Se 7 § äldre FL som i huvudsak oförändrad har förts över till 10 § nuvarande FL och avsnitt 3.2.

[6] Prop. 1985/86:80 s. 57.

[7] Enligt lagmotiven har beträffande 17 § andra stycket FL åsyftats bl.a. det fallet att myndigheten passar på att, utan att överlämna materialet, visa detta för parten i samband med att denne besöker myndigheten av någon annan anledning. Samtidigt har påpekats att denna form av underrättelse bör användas med viss försiktighet, så att kravet på säkerhet inte eftersätts (prop. 1985/86:80 s. 67). Avsikten med föreskriften i 21 § tredje stycket FL har enligt motiven varit att markera att underrättelsen ofta kan ske i en enklare och billigare form än genom delgivning enligt delgivningslagen (a. prop. s. 72).

[8] Se bl.a. SOU 1992:110 s. 460 med hänvisningar.

fjärrskriftsmeddelande.[9] Detta bör jämföras med de nyligen gjorda ändringarna i RB, enligt vilka en part som vill överklaga en tingsrätts dom skall göra detta "skriftligen". Samtidigt har emellertid kravet på egenhändig underskrift utmönstrats i syfte att telefaxmeddelanden skall kunna godtas som vadeinlaga.[10] På motsvarande sätt bör 23 § FL förstås så att ett överklagande kan ske också genom en elektronisk handling. Därmed behövs det inte några författningsändringar i denna del.

Jag föreslår inte heller någon ändring i 21 § tredje stycket FL. Begreppet "skriftlig" bör även här anses innefatta elektroniska rutiner. På samma sätt som jag, beträffande elektronisk delgivning, har föreslagit att den som så önskar skall kunna få handlingen översänd på papper (i vart fall som en serviceåtgärd), bör den som vill ta del av ett beslut kunna få det översänt i form av en traditionell pappershandling. I vissa fall torde detta också bli nödvändigt av praktiska skäl, t.ex. i samband med en begäran om verkställighet då en *vidimerad* papperskopia av beslutet torde behöva företes hos kronofogdemyndigheten, i vart fall så länge besluten inte är digitalt signerade och kan äkthetsprövas med kronofogdemyndighetens tekniska hjälpmedel.

I FL används alltså som framgått begreppet skriftlig i flera bestämmelser och jag har inte funnit anledning att föreslå någon ändring i denna del. Ett ytterligare skäl för att behålla detta begrepp är behovet av att kunna skilja tal och samtal från kommunikation med text som ställs samman i meningar och stycken så att meddelandet koncentreras och tydliggörs.[11] Elektroniska handlingar får på så sätt en utformning som är lämpad för ärendehandläggning. Enskilda och myndigheter bör inte utan närmare överväganden få övergå från att kommunicera med text till att kommunicera med tal. En sådan förändring skulle föra med sig såväl praktiska som administrativa svårigheter, och gränsen mellan skriftlig handläggning respektive handläggning vid sammanträden kunde komma att bli flytande.[12]

[9] Hellners/Malmqvist, Nya Förvaltningslagen, 4 u., s. 300 f., med hänvisningar.

[10] Se t.ex. 50 kap. 1 och 4 §§ RB samt prop. 1993/94:190 s. 108; jfr NJA 1991 s. 407.

[11] Eventuellt i förening med bilder eller grafiska framställningar som kompletterar texten.

[12] Utvecklingen på IT-området har inneburit att tal, text och bild enkelt kan hanteras tillsammans, s.k. multimedia. Beroende på mottagarens förmåga (program m.m.) kan fler eller färre av ett dokuments alla egenskaper presenteras. Har myndigheten eller den enskilde inget ljudkort kan mottagaren inte lyssna på en inlagd ljudkommentar, har mottagaren inte rätt verktyg för videopresentation kan han inte se en videobilaga, etc. Vidare torde långa "muntliga inlagor" bli tidskrävande att avlyssna och att hantera i övrigt, och beslutande myndigheter och enskilda skulle av praktiska skäl bli tvungna att själva överföra åtminstone vissa delar av meddelandet till text.

5.4 Området utanför FL

En allmän lag som FL kan inte anpassas för alla typer av ärenden. Därför har det i 3 § FL föreskrivits att bestämmelser i annan lag eller i förordning som avviker från en föreskrift i FL skall ha företräde. Frågan är då i vilken omfattning den förvaltningsrättsliga regleringen utanför FL är baserad på uttryck som är svåra att tolka eller att annars tillämpa vid elektronisk dokumenthantering.

Det finns en mängd förfaranderegler som har införts innan det var aktuellt med elektroniska rutiner eller som annars kan antas ha tillkommit utan att IT har beaktats. Frågan är därvid hur de ovan berörda uttrycken med anknytning till pappersbaserad hantering av handlingar bör förstås.

Ordet *skriftlig* synes, i anknytning till förfaranderegler, huvudsakligen användas för att utesluta muntliga rutiner. Att uttrycket vanligtvis inte innefattar krav på underskrift framgår av att det i vissa författningar, där det anges att handlingar skall upprättas skriftligt, också föreskrivs att handlingarna skall underskrivas/undertecknas.[13] I IT-sammanhang brukar dock kraven i förfaranderegler på användning av "skriftliga" rutiner eller "handlingar" sägas innebära att traditionella pappersbaserade handlingar måste användas, även när det inte finns uttryckliga eller underförstådda krav på underskrift. Som tidigare angetts har emellertid en genomgång visat att sådana bestämmelser såvitt avser förfaranderegler vanligtvis tolkas så att telefaxmeddelanden godtas, när mottagaren inte finner anledning till tvekan om en handlings äkthet.[14]

När det krävs att en handling skall vara *"undertecknad"* innefattas emellertid inte elektroniska rutiner.[15] Detta formkrav förekommer i en mängd författningar.[16] Enligt min mening bör digitala dokument (dvs.

[13] Se t.ex. 10 § DL, 2 § tredje stycket lagen (1946:807) om handläggning av domstolsärenden, 9 § lagen (1963:197) om allmänt kriminalregister, 7 § lagen (1982:352) om rätt till fastighetsförvärv för ombildning till bostadsrätt, 2 kap. 1 § konkurslagen (1987:672), 2 § lagen (1989:31) om förvaltning av vissa samägda jordbruksfastigheter, 19 § lagen (1990:746) om betalningsföreläggande och handräckning, 2 kap. 1 § andra stycket utsökningsbalken; jfr första stycket andra meningen, 42 kap. 1 § och 2 § tredje stycket RB och 11 § lagen (1994:308) om bostadstillägg till pensionärer.

[14] Beträffande vissa andra typer av regler, t.ex. vid ADB-revision enligt taxeringslagen, har författningsändringar ansetts behövliga, medan andra regler, t.ex. äldre regler om offentlighetsinsyn, har tolkats så att även elektroniska handlingar innefattades (RÅ 1965 ref. 25 och 1971 ref. 15).

[15] Telefaxmeddelanden har i praxis inte ansetts uppfylla RB:s krav på att handlingen skall vara egenhändigt undertecknad genom att det i kravet på egenhändigt undertecknande också har ansetts ligga ett krav på att det är just det undertecknade exemplaret som skall ges in till domstolen (prop. 1993/94:190 s. 108).

[16] En databaserad sökning i Rättsbanken visade att orden "underskriv-" och "underteckna-" förekommer i 100 resp. 462 författningar medan "skriftlig-" förekommer i 1 095 författningar.

elektroniska handlingar med digital signatur eller stämpel) i sådana fall kunna användas på motsvarande sätt som traditionella handlingar med underskrifter, så att behovet av skydd för meddelandenas äkthet tillgodoses. Förutsättningar för sådana rutiner saknas endast när en viss rättighet eller skyddsfunktion knyts till ett unikt fysiskt exemplar, något som knappast förekommer i förvaltningsrättens förfaranderegler.

Databaserade sökningar i Rättsbanken efter författningar där "undertecknad", "underskriven" och "original" förekommer har visat att antalet regler *i lag* som gäller förvaltningsmyndigheters handläggning av ärenden eller domstolars handläggning av förvaltningsärenden inte är särskilt stort. Det förekommer visserligen lagregler som anger formkrav för handlingar som ges in till en myndighet[17] eller som anger att tjänstemän skall underteckna vissa handlingar.[18] Vidare finns regler där begreppet "original" används. Såvitt framgår av min genomgång[19] är det emellertid endast ett begränsat antal regler *i lag* som uppställer krav på användning av traditionella undertecknade pappershandlingar. Enligt vissa regler "får" myndigheten begära bekräftelse genom en i original undertecknad handling.[20] Sådana regler hindrar emellertid, som framgått, inte en användning av elektroniska rutiner när sådana rutiner är lämpliga. Vidare synes uttrycket "original" i lagregler ofta användas i sammanställningen "original eller (bestyrkt) kopia/avskrift".[21]

[17] Ansöknings eller besvärshandlingar enligt 3 § FPL och 13 § vallagen (1972:620), anmälan enligt 11 § religionsfrihetslagen (1951:680) om utträde ur svenska kyrkan, begäran om registerutdrag enligt 10 § DL, skriftlig ansökan enligt 2 § tredje stycket lagen (1946:807) om handläggning av domstolsärenden, hembud enligt 7 § lagen (1982:352) om rätt till fastighetsförvärv för ombildning till bostadsrätt, anmälan till en inskrivningsmyndighet enligt 2 § lagen (1987:232) om sambors gemensamma hem eller enligt 2 § lagen (1989:31) om förvaltning av vissa samägda jordbruksfastigheter, ansökan enligt 2 kap. 1 § konkurslagen och 2 § lagen (1989:31) om förvaltning av vissa samägda jordbruksfastigheter, en skriftlig ansökan enligt 19 § lagen (1990:746) om betalningsföreläggande och handräckning, ansökan eller överklagande enligt 2 kap. 1 § andra stycket och 18 kap. 8 § tredje stycket utsökningsbalken, ansökan enligt 9 § skuldsaneringslag (1994:334), anmälan enligt 20 § lagen (1994:954) om disciplinpåföljd m.m. på hälso- och sjukvårdens område och ansökan enligt 11 § lagen (1994:308) om bostadstillägg till pensionärer.

[18] Protokoll enligt lagen (1939:608) om enskilda vägar, lagen (1973:370) om arbetslöshetsförsäkring och vallagen (1972:620).

[19] Någon fullständig genomgång, utan begränsningar till vissa sökord, har inte varit möjlig i detta sammanhang.

[20] Se mina förslag till ändringar i 33 kap. 3 § RB, 44 § FPL och 10 § FL; jfr 15 kap. 6 § mervärdesskattelagen (1994:200), 4 kap. 10 § taxeringslagen (1990:324), 87 § uppbördslagen (1953:272), 20 kap. 10 § fastighetstaxeringslagen (1979:1152), 54 § lagen (1984:668) om uppbörd av socialavgifter från arbetsgivare och 4 kap. 4 a § lagen (1984:151) om punktskatter och prisregleringsavgifter.

[21] Lagen (1985:193) om internationell järnvägstrafik, lagen (1986:1042) om verkställighet av vissa utländska beslut om rättegångskostnader, delgivningslagen (1970:428), lagen (1976:108) om erkännande och verkställighet av utländskt avgörande angående underhållsskyldighet, lagen (1983:368) om erkännande och verkställighet av österrikiska domar på privaträttens område, lagen (1985:658) om arrendatorers rätt att förvärva arrendestället, äktenskapsbalken, konkurslagen, lagen (1990:746) om betalningsföreläg-

Däremot innefattar många *förordningar* krav på att enskilda och tjänstemän undertecknar handlingar. Till detta kommer bestämmelser där begrepp som "handling" eller"skriftlig" förekommer, varvid tvekan kan uppkomma om elektroniska rutiner innefattas.

5.5 Mitt förslag

Det finns ett antal författningar som innehåller uttryck som innebär att elektroniska rutiner utesluts eller som kan föranleda tvekan till följd av ordvalet. Jag föreslår därför en bestämmelse i lag om att förfaranderegler i andra lagar som gäller förvaltningsmyndigheters handläggning av ärenden eller domstolars handläggning av förvaltningsärenden, där krav ställs på att uppgifter skall hanteras i form av traditionella handlingar, skall få uppfyllas genom användning av digitala dokument, eller — när det kan anses tillräckligt — genom användning av elektroniska handlingar utan digital signatur eller stämpel. Syftet är att möjliggöra ett flexibelt införande av elektroniska rutiner inom förvaltningen, så att förfaranderegler inte behöver ändras varje gång en ny tillämpning skall tas i bruk. En sådan bestämmelse kan placeras i FL under rubriken "Allmänna krav på handläggningen av ärenden" (förslaget till 7 a §). Användningen av signerade elektroniska handlingar bör härvid ses som huvudregel, på motsvarande sätt som det vanligtvis är självklart att pappershandlingar undertecknas. Kravet bör emellertid inte vara absolut, eftersom rutiner där en sådan säkerhet inte behövs bör undantas från de kostnader som kan vara förenade med säkra elektroniska rutiner.

Jag föreslår att regleringen utformas så att regeringen får föreskriva att digitala dokument eller elektroniska handlingar utan digital signatur eller stämpel får användas, om en bestämmelse i lag om handläggning av förvaltningsärenden föreskriver att handlingar skall vara egenhändigt undertecknade eller annars uppställer krav som medför att elektroniska handlingar inte kan användas. Tanken är att regeringen skall kunna bemyndiga berörda statliga förvaltningsmyndigheter att utfärda sådana föreskrifter. Den föreslagna regleringen ger även möjlighet för regeringen att i förordning ge statliga och kommunala myndigheter rätt att besluta om sådana undantag för enskilda fall. På så sätt blir det möjligt för regeringen att på skilda områden överväga om de krav som bör ställas på säkerhet och teknikval är uppfyllda. I det skede när en myndighet överväger en framställning till regeringen om författningsändringar bör det nämligen finnas nödvändigt underlag för att ge närmare besked om de planerade rutinerna.

gande och handräckning, utsökningsbalken och sjölagen; jfr dock de ovan berörda lagreglerna om bekräftelse genom underskriven handling.

Som tidigare anförts bör regleringen inte utformas så att enskilda får ställa krav på en myndighet att godta vissa elektroniska handlingar, trots att myndigheten saknar tillräckliga rutiner för sådan kommunikation.

I 3 § FL föreskrivs att bestämmelser i annan lag eller i förordning som avviker från en föreskrift i FL skall ha företräde. Den bestämmelse jag föreslår (7 a § FL) syftar emellertid just till att regeringen skall få meddela föreskrifter som avviker från en bestämmelse i en annan lag. Om riksdagen skulle anse att ett krav i en lag på användande av traditionella handlingar bör ligga fast, måste det därför i den lagen uttryckligen skrivas in att den föreslagna bestämmelsen i FL inte gäller.

5.6 Normgivningskompetensen och den föreslagna bestämmelsen

Förslaget att regeringen skall ha rätt att bemyndiga berörda myndigheter att föreskriva att krav på traditionella skriftliga rutiner får uppfyllas elektroniskt, är förenligt med bestämmelserna om normgivningsmaktens fördelning. De aktuella förfarandereglerna faller i princip inom ramen för regeringens restkompetens, och att regeringen får överlåta åt underordnad myndighet att meddela bestämmelser i ämnet följer av 8 kap. 13 § RF. Normgivningen har emellertid, som framgått, i vissa delar skett i lag (8 kap. 14 § RF). En ändring i denna del skall alltså ske genom lag (8 kap. 17 § RF). Jag har därför föreslagit att bestämmelsen förs in i FL. En sådan regel — att undantag från krav i lag på användning av traditionella pappershandlingar får föreskrivas på lägre nivå än genom lag — kan visserligen ge intryck av att det skulle vara fråga om delegation av riksdagens normgivningskompetens. Bestämmelsen innebär emellertid endast att riksdagen återlämnar till regeringen att utöva sin restkompetens.[22]

Mitt förslag rör också förfarandet vid kommunala förvaltningsmyndigheter. Formerna för dokumentation vid ärendehandläggning utgör emellertid inte sådana kommunalrättsliga frågor som enligt 8 kap. 5 § RF måste regleras i lag.

Möjligheten att låta krav på användning av traditionella handlingar uppfyllas genom IT-rutiner avser bara regler om förvaltningsmyndigheters handläggning av ärenden eller domstolars handläggning av förvaltningsärenden, dvs. förfaranderegler som faller inom ramen för regeringens restkompetens. Härvid bör uppmärksammas att vissa

[22] Det sägs inget i RF om möjligheterna att delegera normgivningsmakt till regeringen eller andra myndigheter genom bemyndigande i lag som riksdagen har stiftat med stöd av 8 kap. 14 § RF. Sådana bemyndiganden förekommer dock (jfr Strömberg, Normgivningsmakten, 2 u., s. 98 och prop. 1995/96:84 s. 8).

lagregler har ett "blandat" innehåll. Det kan vara fråga om t.ex. en förfaranderegel som visserligen faller inom ramen för regeringens restkompetens, men som också inrymmer åligganden för enskilda enligt 8 kap. 3 § RF. Den föreskriftsrätt som regeringen får genom den föreslagna regeln i FL omfattar endast sådana föreskrifter som faller inom ramen för restkompetensen. Som exempel på regler som alltså faller utanför den bestämmelse jag har föreslagit kan nämnas uttrycken "skriftligt meddelande" och "skriftlig uppgift" i bestämmelser om skattetillägg och förseningsavgift, eftersom regleringen innebär åligganden för enskilda enligt 8 kap. 3 § RF.[23]

[23] Se bl.a. 5 kap. 1 och 4 §§ taxeringslagen (1990:324), 7 kap. 1 och 4 §§ lagen (1984:151) om punktskatter och prisregleringsavgifter, 18 kap. 1 och 5 §§ mervärdesskattelagen (1994:200) och 38 § lagen (1984:668) om uppbörd av socialavgifter från arbetsgivare; jfr Strömberg, a.a., s. 77.

6 Övriga frågor

6.1 Offentlighetsinsynen

Handlingar (inkl. upptagningar) är enligt huvudregeln i tryckfrihetsförordningen *allmänna* om de förvaras hos en myndighet och är att anse som inkomna eller upprättade där.

En upptagning anses vara *förvarad* hos myndigheten om upptagningen är tillgänglig för myndigheten för överföring i sådan form att den kan läsas, avlyssnas eller på annat sätt uppfattas. Även om en sådan överföring är faktiskt möjlig anses en upptagning i ett personregister emellertid inte vara förvarad hos en myndighet om myndigheten saknar rättslig befogenhet att göra överföringen (2 kap. 3 § TF).[24]

Frågan om när en upptagning skall anses *inkommen* har samordnats med förvaringsrekvisitet (2 kap. 6 § TF) så att en upptagning anses inkommen till en myndighet när "annan" — ett offentligt organ eller ett privaträttsligt subjekt — "har gjort den tillgänglig för myndigheten" på sätt som anges i 2 kap. 3 § andra stycket.

Meddelanden som blir tillgängliga för en myndighet eller som expedieras från en myndighet via t.ex. elektronisk post blir således allmänna handlingar enligt reglerna i TF. Behovet av att upprätthålla ett naturligt samband mellan vad som är en allmän handling enligt TF respektive en inkommen handling enligt FL, och att i övrigt kunna samordna de krav som ställs på elektroniska rutiner, har berörts i flera sammanhang.[25] Den traditionella regleringen bygger emellertid som huvudregel på handlingens fysiska belägenhet, medan regleringen i TF avseende upptagningar har inriktats på frågan om handlingen — oberoende av var den fysiskt lagras — är tillgänglig för överföring till läsbar form.

[24] Undantag föreskrivs vidare bl.a. för upptagningar som förvaras hos en myndighet endast som ett led i teknisk bearbetning eller teknisk lagring för annans räkning (2 kap. 10 § TF), och för brev, telegram eller annan sådan handling som har lämnats in till eller upprättats hos myndigheten endast för befordran av meddelande (2 kap. 11 § första stycket 1 TF). Vidare föreskrivs att handling som ingår i bibliotek inte skall anses som allmän. Detta undantag tillämpas emellertid inte på upptagningar i sådant register som myndighet har tillgång till enligt avtal med annan myndighet (2 kap. 11 § första stycket 3 och andra stycket TF).

[25] Se Hellners/Malmqvist, Nya förvaltningslagen, 4 u., s. 104 och SOU 1989:20 s. 101.

Frågor om *registrering av allmänna handlingar* regleras i 15 kap. sekretesslagen (1980:100). En handling som har kommit in till eller upprättats hos myndighet skall registreras utan dröjsmål, om det inte är uppenbart att den är av ringa betydelse för myndighetens verksamhet.[26] Vid en användning av datorer som är anslutna till nät aktualiseras frågan om dessa bestämmelser skall tillämpas också på t.ex. en extern databas som, kanske av en händelse, har blivit tillgänglig för en myndighet via nätet, trots att myndigheten aldrig avser att använda denna databas; jfr avsnitt 11.9.

Enligt motiven till nuvarande reglering av handlingsoffentligheten är det en naturlig utgångspunkt att så långt som möjligt dra en parallell med den ordning som gäller för konventionella handlingar. Regleringen synes emellertid inte vara anpassad till sådan fri åtkomst till omfattande datamängder som kännetecknar nuvarande strukturer på IT-området.[27] Genom att en upptagning, med vissa undantag för personregister, kan ses som allmän handling hos en myndighet redan genom att myndigheten faktiskt disponerar över möjligheten att överföra upptagningen till läsbar form, uppkommer frågan om det är en riktig tolkning av TF som — ofta i skämtsamma ordalag — förs fram, när det aktualiseras hur rekvisiten "inkommen" och "förvarad" bör tillämpas på upptagningar som är åtkomliga via t.ex. Internet.[28] Skall verkligen alla databaser som är tekniskt tillgängliga som en följd av att en myndighet är uppkopplad mot datanät, med undantag för sådana som omfattas av den så kallade biblioteksregeln i 2 kap. 11 § TF, anses vara tillgängliga för offentlighetsinsyn hos myndigheten?

Det är inte min uppgift att överväga ändringar i grundlag. Frågan är emellertid om den berörda tolkningen av TF är riktig beträffande upptagningar i databaser som visserligen är tekniskt tillgängliga för

[26] Registrering får emellertid underlåtas beträffande allmänna handlingar som inte är sekretessbelagda, om handlingarna hålls så ordnade att det utan svårighet kan fastställas om handlingarna har kommit in eller upprättats. Vidare finns ett undantag beträffande upptagningar som förs in i ett register som är tillgängligt för flera myndigheter. Endast den myndighet som gör införingen är registreringsskyldig (15 kap. 1 och 13 §§ sekretesslagen).

[27] I motiven nämns inget om den nu aktuella situationen där handlingar blir tillgängliga för myndigheter utan att den som tillhandahåller en databas har en tanke på att göra upptagningar tillgängliga för en viss myndighet. Vanligtvis har myndighetens överenskommelse med ett företag som tillhandahåller nätanslutningen inget samband med de databaser som tillhandahålls i större, kanske världsomspännande nät. Myndigheter avser vanligtvis endast att sända och ta emot meddelanden. Den nättjänst och de programvaror som myndigheten har kan emellertid ge tekniska möjligheter att få tillgång till omfattande datamängder. Jfr dock den översyn av offentlighetsprincipen som har gjorts av Data- och offentlighetskommittén i dess slutbetänkande Integritetsskyddet i informationssamhället 5 (SOU 1988:64).

[28] Se bl.a. Bohlin, Allmänna handlingar, s. 119.

myndigheten men som ändå inte rimligen kan sägas ingå i något allmänt organs informationstillgångar.[29]

Härvid blir bestämmelsen i 6 § av betydelse. Enligt lagtextens ordalydelse är en upptagning inkommen till en myndighet "när annan har gjort den tillgänglig för myndigheten på sätt som angives i 3 § andra stycket". Åtgärden varigenom upptagningen görs tillgänglig måste alltså enligt bestämmelsens ordalydelse — för att upptagningen skall anses inkommen — ha vidtagits av "annan"[30], och denne skall ha gjort upptagningen tillgänglig "för myndigheten".[31] Om bestämmelsen tolkas så att det är tillräckligt med en teknisk möjlighet för myndigheten att hämta handlingen till sitt system, skulle en myndighet vara skyldig att, för offentlighetsinsyn, göra tillgängliga även upptagningar i databaser som myndigheten helt saknar samröre med och upptagningar som det är otänkbart att myndigheten annars skulle hämta till sitt informationssystem, t.ex. därför att uppgifterna är brottsliga eller att det utgör brott att sprida dem.[32] Det skulle därmed vidare bli praktiskt omöjligt för myndigheten att veta vilket material som hör till myndighetens informationstillgångar.

Enligt min mening är det inte rimligt att tolka bestämmelsen på detta sätt. Visserligen har "annan" genom inkoppling gjort databasen tillgänglig — vanligtvis för alla som är anslutna till det aktuella nätet — men att hävda att annan redan härigenom har gjort upptagningarna i databasen tillgängliga "för myndigheten", framstår inte som en naturlig tolkning och leder långt bort från den avsedda samordningen med vad som gäller för konventionella handlingar och från offentlighetsinsynens syften. Denna bedömning innebär bl.a. att sådana upptagningar inte behöver diarieföras enligt 15 kap. sekretesslagen (1980:100). Dessa frågor övervägs emellertid av kommittén om ny datalag m.m. (Ju 1995:08, dir. 1995:91).

[29] Jfr prop. 1975/76:160 s. 87 där undantagsregler rörande upptagningar hos en myndighet som endast har en teknisk uppgift har motiverats med att sådana upptagningar inte rimligen kan sägas "ingå i de allmänna organens informationstillgångar".

[30] Vem denne skall vara klargörs inte i lagmotiven, men begreppet kan inte — rent språkligt — förstås på annat sätt än såsom avseende någon utomstående, t.ex. en annan myndighet eller ett privat dataföretag (Bohlin, Allmänna handlingar, 1988, s. 119).

[31] I den allmänna motiveringen har den nya regleringen för upptagningar beskrivits som en övergång från var handlingen fysiskt förvaras till *förfogandet* — ordet taget i allmän betydelse — över en upptagning, och i specialmotiveringen behandlas frågan i anknytning till åtgärder som andra utför *för myndighetens räkning* (prop. 1975/76:160 s. 88 och 137).

[32] Som exempel på ytterligheter kan nämnas handlingar tillgängliga via Internet som fysiskt förvaras i datorer i avlägsna länder och på språk som myndigheten knappast kan förstå, och som kan utgöras av sådana "brottsliga upptagningar" som behandlas i avsnittet om elektroniska förmedlingstjänster, eller sådana programvaror för kryptering, som kan hämtas i en databas i ett land där förbud föreskrivits mot export av programvaran.

6.2 Sekretess för koder m.m.

Bestämmelserna i sekretesslagen (1980:100) gäller oberoende av om en myndighet förvarar uppgifter på papper eller elektroniskt. Regleringen kan alltså tillämpas även vid en övergång till elektronisk dokumenthantering. De rättsliga komplikationer som framträder i IT-miljön sammanhänger i stället med t.ex. nya möjligheterna att kommunicera via nät och organisatoriska förändringar.[33] Dessa frågor får dock tas upp i ett vidare sammanhang.

En fråga har emellertid direkt anknytning till de regler jag föreslår för digitala dokument. En användning av sådana dokument på myndighetsområdet förutsätter att nycklar och anknytande uppgifter för digital signering och autenticering samt för sekretesskydd kan skyddas mot insyn.[34]

Enligt 5 kap. 2 § sekretesslagen gäller sekretess för uppgift om säkerhetsåtgärd med avseende på bl.a. telekommunikation (punkt 3) och behörighet att få tillgång till upptagning för ADB eller annan handling (punkt 4), om det kan antas att syftet med åtgärden motverkas om uppgiften röjs. Enligt 3 § samma kapitel gäller sekretess också för uppgift som lämnar eller kan bidra till upplysning om chiffer, kod eller liknande metod som har till syfte att underlätta befordran eller användning i allmän verksamhet av uppgifter utan att föreskriven sekretess åsidosätts, om det kan antas att syftet med metoden motverkas om uppgiften röjs.

I den mån s.k. aktiva kort eller liknande utrustning används så att signering m.m. sker i kortet eller annan utrustning utan att nyckeln exponeras, torde nyckeln inte anses vara förvarad hos myndigheten eftersom den inte är tillgänglig för myndigheten med tekniskt hjälpmedel som myndigheten själv utnyttjar för överföring i sådan form att den kan läsas, avlyssnas eller annars uppfattas (2 kap. 3 § TF).

När nyckeln är tillgänglig för överföring i uppfattbar form är den visserligen en allmän handling men den är sekretessbelagd om den används på sätt som sägs i 5 kap. 3 § sekretesslagen. Används den för informationssäkerhet vid telekommunikation i t.ex. ett allmänt datanät

[33] I princip skall en sekretessprövning ske för varje enskilt utlämnande, medan vissa myndigheter vill tillhandahålla information för direktåtkomst, via nät. Dessutom kan programvaror ge möjligheter för enskilda att med olika kombinationer av söknycklar sammanställa nya (potentiella) handlingar, varvid frågan om sekretess beträffande dessa nya uppgiftskonstellationer aktualiseras. Det förekommer också strävanden efter rationaliseringar där myndigheter t.ex. lagrar och behandlar data med gemensamma resurser eller annars organiserar verksamheten på ett sätt som kan vara svårt att förena med regleringen i sekretesslagen, se vidare LEXIT-rapporten s. 27 f.

[34] Se närmare bilaga 2 angående utformningen av sådana rutiner.

eller i s.k. behörighetskontrollsystem kan i stället 5 kap. 2 § sekretess lagen tillämpas.[35]

Beträffande säkerhetsåtgärder som är inriktade endast på att verifiera om en handling härrör från angiven utställare — utan att samtidigt bereda sekretesskydd, skydd för telekommunikation eller skydd för åtkomst till ADB-upptagningar — torde det emellertid inte finnas någon tillämplig bestämmelse om sekretess. Detsamma gäller om hemliga koder m.m., utan att en viss utställare pekas ut, används för att skydda vissa datamängder mot manipulation.[36] Behovet av skydd är härvid uppenbart. Jag föreslår därför en bestämmelse om sekretess för koder m.m. som har till syfte att göra det möjligt att kontrollera om uppgifter har förvanskats (förslaget till ändring i 5 kap. 3 § sekretesslagen). Regeln avses innefatta både koder som syftar till att verifiera om uppgifter härrör från angiven utställare och koder som syftar endast till att skydda vissa datamängder. Som exempel på koder av det senare slaget kan nämnas tekniska skydd mot förändringar i programvaror eller andra datamängder som är betydelsefulla från tekniska eller andra utgångspunkter.

6.3 Skyddet för persondata

I datalagen (1973:289) ges skydd mot otillbörligt intrång i den enskildes personliga integritet till följd av att personuppgifter registreras med hjälp av ADB. *Personregister* definieras enligt 1 § datalagen (DL) som register, förteckning eller andra anteckningar som förs med hjälp av automatisk databehandling och som innehåller personuppgift som kan hänföras till den som avses med uppgiften. Personregister får enligt 2 § DL inrättas och föras endast av den som har anmält sig hos Datainspektionen och fått bevis om detta, s.k. *licens*. Om personregistret skall innehålla vissa känsliga uppgifter som generellt sett kan antas medföra risk för otillbörligt intrång i enskilds personliga integritet, t.ex. politisk åskådning, värderingar och omdömen, behövs också *tillstånd* av Datainspektionen.

Av 1 § DL följer att den för vars verksamhet ett personregister förs är *registeransvarig*, om han förfogar över registret. Den som har möjlighet och befogenhet att överföra registret till läsbar form och som kan påverka registrets innehåll anses förfoga över registret. Den registeransvarige åläggs enligt datalagen att inrätta och föra personregister så att otillbörligt intrång i registrerades personliga integritet inte uppkommer. Därvid skall särskilt iakttas att registret förs för ett *bestämt*

[35] Hans Corell m.fl., Sekretesslagen, 3 u., s. 122.

[36] Skulle en sådan kod lämnas ut kunde den som fick tillgång till koden manipulera uppgifter så att skyddet mot förvanskning inte ger utslag.

ändamål, och insamling, registrering, utlämnande och användning av uppgifter skall ske i överensstämmelse med registrets ändamål. I motiven till datalagen tas avstånd från vitt bestämda ändamål av typen "diskussionsklubb". Vidare skall *uppgifterna skyddas* mot otillåten spridning (7 § första stycket 5 DL).

Andra bestämmelser, som bygger på att den registeransvarige har kontroll över informationsbehandlingen så att han kan bestämma vad registret skall innehålla, är föreskrifterna om skyldighet att *rätta, ändra, utesluta* (8 §) och *komplettera* (9 §) registrerade uppgifter som är oriktiga, missvisande eller ofullständiga. Den registeransvarige är också skyldig att på begäran av en enskild *underrätta* denne om personuppgifter som ingår i personregistret och innefattar upplysning om honom (10 § DL).

För den händelse en registrerad tillfogas skada genom att ett personregister innehåller oriktiga eller missvisande uppgifter om honom har den registeransvarige ett strikt *skadeståndsansvar* (23 § DL).

Datalagen har setts över i olika etapper, och regeringen har nyligen tillsatt en parlamentarisk kommitté (dir. 1995:91) med uppgift att bl.a. anpassa regleringen till EG:s dataskyddsdirektiv.

Skyddet för persondata tillgodoses vidare genom s.k. registerlagar, och det är i sådana lagar som nya regler har införts för elektronisk dokumenthantering inom skatteförvaltningen och exekutionsväsendet. Skatteregisterlagen (1980:343) och utsökningsregisterlagen (1986:617) har ändrats så att särskilda regionala register tillskapats för elektroniska akter och anknytande referensregister (jfr diarium) samt administrativa och tekniska uppgifter m.m.[37] Härvid skyddas den enskilde inte bara genom att registren gjorts länsvisa i stället för rikstäckande utan också genom begränsningar av åtkomsten till registren (lokal åtkomst) och av de sökbegrepp som får användas.[38] Den ökade registreringen av personuppgifter har på så sätt mötts med åtgärder för att skydda den enskilde.

De regler jag har föreslagit för elektronisk dokumenthantering syftar till att alla elektroniska handlingar som en part ger in och som en myndighet upprättar i ett visst ärende skall få bevaras elektroniskt i en akt så att varje handling kan göras läsbar med det innehåll den har

[37] Se prop. 1994/95:93 och 1994/95:168.

[38] Begränsningar av sökbegrepp har stöd i 2 kap. 3 § andra stycket TF, om upptagningen ingår i personregister och myndigheten enligt lag eller förordning, eller särskilt beslut som grundar sig på lag, saknar befogenhet att göra överföringen till läsbar eller annars uppfattbar form. Omfattande begränsningar av sökbegrepp i syfte att skydda persondata aktualiserar emellertid den principiella frågan om vilka inskränkningar i rätten till offentlighetsinsyn med avseende på s.k. potentiella handlingar som bör godtas (jfr 2 kap. 3 § andra stycket RF). Denna fråga faller dock inom ramen för den översyn av TF som pågår i annan ordning (Ju 1995:08).

givits av utställaren.[39] I samband med införandet av elektroniska akter inom skatte- och exekutionsväsendet aktualiserades frågan om handlingar som scannas eller annars bevaras och används så att de kan visas på bildskärm eller skrivas ut, men inte så att sökningar m.m. blir möjliga, är att bedöma som personregister. Det ansågs därvid stå klart att de elektroniska akterna bör anses utgöra personregister i datalagens mening.[40] På motsvarande sätt torde de nya IT-baserade tillämpningarna på vilka mina förslag avses bli tillämpliga få ett sådant innehåll och ändamål att akterna i förening med de diarieliknande uppgiftssamlingar som behövs för att hantera de elektroniska akterna utgör personregister.

I anknytning till elektronisk överföring av handlingar mellan informationssystem aktualiseras frågan om vem som bör anses vara *registeransvarig* när en stor mängd användare kan påverka innehållet i ett register. De som ger in elektroniska handlingar till en myndighet påverkar visserligen på sätt och vis innehållet i myndighetens register. Ingivaren blir emellertid inte därmed att anse som registeransvarig; jfr att den som via knapptelefon gör en sjukanmälan till en försäkringskassas informationssystem eller en transaktion med en banks informationssystem inte därmed blir att anse som registeransvarig för det av kassan respektive banken förda personregistret.

Regleringen i DL bygger på att personregister förs för ett bestämt ändamål och att dataregistreringen begränsas till vissa uppgifter som har valts ut.[41] I de elektroniska akterna avses emellertid hela handlingar bevaras så som de ursprungligen har ställts ut och syftet är att handläggare och enskilda skall kunna ta fram och läsa dess handlingar — inte att sammanställa nya uppgiftskonstellationer. Härvid begränsas möjligheten att förutse vilka uppgifter som kan komma att finnas i en elektronisk akt eftersom ett sådant register avses innefatta samtliga handlingar från anhängiggörande till beslut, och innehållet i dessa handlingar kan inte förutses. Även *känsliga personuppgifter* (jfr 4 § och 6 § andra stycket DL) som förekommer i en elektronisk handling måste kunna lagras på samma sätt som handlingen i övrigt. Enskilda bör vara oförhindrade att genom uppgifter i handlingar ta tillvara sin rätt och myndigheterna bör få motivera sina beslut även om integritetskänsliga uppgifterna därigenom registreras.

Regleringen i DL bygger på att den registeransvarige har full kontroll över databehandlingen, en situation som självklart förelåg vid

[39] Rutinerna är parallella med pappersbaserade förfaranden och det är en självklarhet att handlingarna i en akt inte får ändras, såväl enligt bestämmelserna om brott mot urkunder i 14 kap. BrB (jfr SOU 1992:110 s. 229 f.) som föreskrifterna i 2 kap. TF om allmänna handlingars offentlighet.

[40] Se Ds 1994:80 s. 124 f. med hänvisningar.

[41] Uppgifterna registreras vanligtvis i konstellationer som avviker från de handlingar som ligger till grund för registreringen, och de tekniska rutinerna gör det möjligt att skapa nya sammanställningar av uppgifter, s.k. potentiella handlingar.

datalagens tillkomst. När uppgifter i mål och ärenden skall kunna ges in elektroniskt synes ett sålunda utformat registeransvar — om inga undantag föreskrivs — förutsätta någon form av granskning av varje elektronisk handling för att bedöma om den får tas in i registret. En sådan förhandsgranskning är dock svår att genomföra, och svår att förena med syftet bakom övergången till elektronisk hantering av dokument och akter på förvaltningsområdet. Begränsningar genom ändamålsbeskrivningar och genom angivelser av vilka uppgifter som får registreras blir därmed inte tillräckligt verksamma.[42] Jag förordar därför begränsningar av det slag som har införts på bl.a. skatteområdet.[43] Eftersom datalagen är föremål för översyn i annan ordning föreslår jag ingen reglering i denna del. När myndigheter inför elektronisk dokumenthantering med elektroniska akter kan emellertid nya register antas uppkomma. Därmed bör myndigheten — även om andra register vid myndigheten regleras i lag — vanligtvis kunna ansöka om Datainspektionens tillstånd att föra det nya registret. I övriga fall krävs författningsändringar.

Avsikten att bevara de elektroniska handlingarna med det innehåll utställaren har givit dem aktualiserar frågan om hur bestämmelserna om *rättelse m.m.* bör tillämpas.[44] Det torde normalt saknas anledning att anta att risken för otillbörligt intrång i en registrerads personliga integritet, om en felaktig uppgift har tagits in i en elektronisk akt, är större än vid pappersbaserad hantering av uppgifter.[45] Som ett undantagsfall vid bedömningen av frågan om en uppgift är att anse som oriktig eller missvisande har också nämnts register vars ändamål är att återge det exakta innehållet i ett visst dokument.[46] De här aktuella akterna avses innehålla endast inkomna och upprättade handlingar och dessa skall skyddas mot ändringar. Åtgärder för rättelse eller ändring av en sådan handling skulle leda till att den av avsändaren utställda handlingen får ett annat innehåll än han har avsett; jfr om en handläggare skulle ändra innehållet i de pappersurkunder som finns i en

[42] Innehållet i de diarieliknande register som knyts till akterna bör emellertid i huvudsak begränsas till sådana kortfattade uppgifter som behövs för att identifiera ärendet, parter och andra berörda samt de handlingar som hör till ärendet; jfr pappersbaserade dagboksblad där uppgifter av känsligt slag vanligtvis inte tas in annat än möjligen i en s.k. tjänsteanteckning.

[43] Alternativen synes bli att förbjuda elektronisk akthantering, eftersom känsliga uppgifter kan förekomma, eller att bortse från de ökade riskerna för otillbörligt intrång i den enskildes personliga integritet.

[44] Dessa bestämmelser har samband med risken för "fortplantning" av fel genom de möjligheter IT för med sig att använda data i olika sammanhang. Det anses i princip vara likgiltigt om de förhållanden som gör att en uppgift är oriktig eller missvisande förelåg redan då uppgiften registrerades eller har inträtt först därefter.

[45] Jfr Ds 1994:80 s. 137. I Regeringens proposition 1994/95:93 Elektronisk dokumenthantering inom skatteförvaltningen, m.m. togs frågan inte upp.

[46] Kring/Wahlqvist, Datalagen, 1989, s. 193 f.

traditionell akt. Om en felaktig uppgift har lämnats i en handling får detta i stället korrigeras genom en kompletterande handling. Beträffande de diarieliknande uppgiftssamlingar (egentliga register) som behövs för hanteringen av elektroniska akter bör dock reglerna om rättelse m.m. kunna tillämpas så att de korrekta uppgifterna förs in direkt i det sammanhang där de hör hemma. Det måste härvid beaktas att de ursprungliga uppgifterna kan utgöra allmänna handlingar och att en radering kan kräva ett beslut om gallring.

Skyldigheten enligt 10 § DL, att på begäran av en enskild underrätta om innehållet i personuppgift om denne, kan vara svår att förena med elektroniska akter eftersom den registeransvarige av integritetsskäl knappast kan tillåtas utforma informationsbehandlingen så att personuppgifter som rör en viss person generellt kan tas fram. Anpassningar av programvaror m.m. för att göra sådana sökningar möjliga skulle kunna användas i motsatt syfte, så att påtagliga risker för otillbörligt integritetsintrång framträder. Det torde därför behövas en särskild reglering för personuppgifter i elektroniska akter.[47] Underrättelser enligt 10 § första stycket DL synes inte kunna uppta uppgifter i handlingar vilka lagras så att de — till följd av tekniska spärrar eller rättsliga begränsningar — inte kan eller får användas för sökningar varigenom uppgifter om den aktuella personen tas fram.[48] Skulle varje enskild uppgift i dessa akter göras sökbara framträder uppenbara risker för otillbörligt integritetsintrång då även känsliga uppgifter torde förekomma.[49]

Det finns även andra invändningar mot fullständiga utdrag avseende elektroniska akter. Sådana utdrag skulle i många fall bli mycket omfattande eftersom alla handlingarna i elektroniska akter som rör en viss person skulle komma att innefattas i utdraget. Vidare skulle det knappast fylla någon funktion att i ett utdrag ta med sådana handlingar som har getts in av den som begär utdraget eller som redan har expedierats till honom.[50] Undantag för sådana handlingar har därför införts för elektroniska akter på skatte- och exekutionsområdet, där det

[47] I samband med skattedatoriseringen yttrade Datainspektionen att frågan borde lagregleras och att det är ett minimikrav att utdragen innehåller specificerade uppgifter som gör att den enskilde kan identifiera de handlingar som enligt utdraget har tillförts registret.

[48] Även om databaserade sökningar tilläts skulle det — eftersom fråga är om text som inte har strukturerats utifrån särskilda kriterier — krävas manuella sammanställningar och selekteringar. Det är nämligen inte säkert att personuppgifterna fångas in genom att t.ex. några rader tas fram före eller efter det att personens namn förekommer. Personuppgifter i texten kan på andra sätt knyta an till den som har begärt ett utdrag.

[49] Det är knappast möjligt att hindra enskilda från att föra in känsliga uppgifter i elektroniska handlingar.

[50] Jfr om den som förekommer i en stor mängd mål eller ärenden skulle ha rätt att kostnadsfritt begära en fullständig kopiering av alla akter rörande honom, trots att han vanligtvis redan har fått del av dessa handlingar.

i princip är tillräckligt att utdraget innehåller den information som behövs för att den som begär uppgiften skall kunna identifiera de handlingar som har förts in i personregistret.

Frågan om hur reglerna i datalagen om bl.a. registerutdrag bör utformas hör visserligen hemma inom kommittén Ny datalag m.m. (dir. 1995:91). Planerna på en snabb övergång till elektronisk dokumenthantering innebär emellertid att kommitténs arbete inte kan avvaktas. Jag föreslår därför en bestämmelse i datalagen (10 a §), i princip efter förebild av 18 § skatteregisterlagen och 10 a § utsökningsregisterlagen.[51] Vid min genomgång av nuvarande reglering har det emellertid framkommit att denna behöver övervägas ytterligare.

Enligt bestämmelsen i skatteregisterlagen omfattar undantaget uppgift i handling som har getts in av enskild eller som den registeransvarige har expedierat till den registrerade. Begränsningen till handling som har getts in *av enskild* är hämtad från en framställning av Riksskatteverket om författningsändringar, men den har inte motiverats närmare. Man kan fråga sig varför en handling som har getts in av annan enskild än den registrerade inte skall tas med, medan motsatsen skall gälla beträffande en handling som har getts in av en myndighet samt hur registerutdrag skall kunna framställas med automatik när sådana gränsdragningar införs. Motsvarande bestämmelse i utsökningsregisterlagen innehåller inte någon sådan begränsning. Denna skillnad kan möjligen ha sin grund i att handlingar på exekutionsområdet mer frekvent ges in från myndigheter.

Begränsningen i gällande rätt till sådana handlingar som den registeransvarige har expedierat *till den registrerade*, fanns inte med i utredningsförslaget rörande elektroniska akter på skatteområdet. Avgränsningen torde leda till att utdragen får framställas manuellt, eftersom en sådan sortering knappast kan ske med automatik.

En undantagsregel för hela myndighetsområdet bör ge utrymme också för hantering av akter som innehåller handlingar som har kommit in från en annan myndighet. Beträffande inkommande handlingar föreslår jag därför samma avgränsning som för exekutionsväsendet.

Beträffande handlingar som upprättas och tillförs akter som rör den registrerade torde vanligtvis bestämmelserna om partsinsyn medföra att nära nog samtliga handlingar expedieras till den registrerade, och det förefaller osannolikt att handlingar med betydelsefulla personuppgifter inte skulle expedieras. Jag föreslår därför inte någon begränsning till handlingar som har expedierats. Vill den enskilde ta del av en handling som inte har expedierats till honom har han rätt till det med stöd av

[51] Prop. 1994/95:93 s. 11, 33 och 45 och prop. 1994/95:168 s. 9, 27 och 30.

offentlighetsprincipen och bestämmelserna om partsinsyn.[52] Sådan åtkomst förutsätter emellertid att den registrerade vet vilka handlingar som finns i akter som rör honom. Därför behövs en bestämmelse som motsvarar andra meningen i 18 § skatteregisterlagen och 10 a § utsökningsregisterlagen.

Regleringen bör emellertid ges en mer lättillgänglig utformning. Uppgifter om vilka handlingar som finns i akter som rör en enskild förs vanligtvis i form av dagboksblad eller liknande sammanställningar, och det torde vara enkelt att, vid en begäran om underrättelse, mångfaldiga och sända ut sådana redan gjorda sammanställningar. Jag föreslår därför den föreskriften att det av registerutdraget skall framgå vilka handlingar som finns i en elektronisk akt som avser den registrerade.[53] Mot en sådan ordning kan möjligen invändas att det kan förekomma att dagboksbladet är mycket omfattande medan den som begär underrättelsen — t.ex. en sakägare i ett stort fastighetsbildningsmål — förekommer endast i en enstaka handling. Här får remissbehandlingen utvisa om mitt förslag, som är inriktat på att förenkla hanteringen och författningsregleringen, skulle kunna leda till att utdragen annat än undantagsvis blir alltför omfattande.

Om mitt förslag genomförs kan bestämmelserna i 18 § skatteregisterlagen och 10 a § utsökningsregisterlagen upphävas.

Slutligen aktualiseras frågan om hur uppgifter om den registrerade som finns i andra akter än dem som avser honom bör behandlas. Frågan tas inte upp i lagmotiven. Bevarande av handlingar i elektroniska akter torde emellertid från integritetssynpunkt förutsätta sådana tekniska eller rättsliga begränsningar att uppgifter om annan än den person som en akt avser inte kan sökas fram med ADB. Därmed torde sådana uppgifter inte utgöra personregister, och alltså inte behöva tas med i ett registerutdrag.

Bestämmelserna i DL om strikt *skadeståndsansvar* för den registeransvarige kan vara svåra att förena med en rätt för enskilda att sända in elektroniska handlingar och behovet av att bevara inkomna handlingar oförändrade. Denna fråga bör dock behandlas i ett vidare sammanhang. Frågan om hur skyldigheten enligt 14 § DL att *tillföra ADB-upptagningar i läsbar form* bör tillämpas vid elektronisk dokumenthantering behandlas i den nämna bilagan angående elektroniska akter m.m. (bilaga 6)[54], medan frågan om utlämnande av persondata

[52] Till skillnad från ett registerutdrag enligt 10 § DL får alltså den enskilde betala en avgift för en utskrift om beställningen överstiger nio sidor, se 15 § avgiftsförordningen (1992:191).

[53] Om ärendehandläggningen sker på elektronisk väg utan att det har tillskapats möjligheter att ta fram registerutdrag av detta slag föreligger inte elektroniska akter i den bemärkelse som avses här (jfr bilaga 6). Därmed blir inte den föreslagna bestämmelsen om undantag från s.k. 10 §-utdrag tillämplig.

[54] Jfr prop. 1994/95:93 s. 34 och Ds 1994:80 s. 138 f.

för automatisk databehandling i *utlandet* behandlas i avd. III om elektroniska förmedlingstjänster.[55]

6.4 Arkivfrågor

Allmänna bestämmelser om myndigheternas arkiv ges främst i arkivlagen (1990:782), arkivförordningen (1991:446) och föreskrifter av Riksarkivet.

Enligt 3 § första stycket arkivlagen bildas en myndighets arkiv av de allmänna handlingarna hos myndigheten. Handlingarna i ett ärende är att anse som arkiverade när ärendet har slutbehandlats. Beträffande diarier, journaler och förteckningar som förs fortlöpande anses dock varje anteckning vara arkiverad i och med att den har införts (3 § arkivförordningen). Det betyder att en upptagning som förs fortlöpande omfattas av arkivlagens bestämmelser redan under aktiv tid. Begreppet arkiv har således i arkivlagen ett något vidare innehåll än i allmänt språkbruk.

Arkivet skall enligt 3 § tredje stycket arkivlagen bevaras, hållas ordnat och vårdas så att det tillgodoser rätten att ta del av allmänna handlingar samt behovet av information för rättskipningen, förvaltningen och forskningen. Detta är den grundläggande bestämmelsen. Av den framgår bl.a. att huvudregeln är att arkiven skall bevaras i sin helhet. Längre fram i lagen föreskrivs undantag från denna regel, framförallt genom bestämmelserna om gallring.

I 5 och 6 §§ arkivlagen ges vissa *basregler* för myndigheternas arkivvård. En myndighet skall vid registreringen av en allmän handling ta hänsyn till dess betydelse för en ändamålsenlig arkivvård och vid framställningen av handlingar använda materiel och metoder som är lämpliga med hänsyn till behovet av arkivbeständighet. Vidare skall myndigheten organisera arkivet på ett sådant sätt att rätten att ta del av allmänna handlingar underlättas, skydda arkivet mot förstörelse, skada, tillgrepp och obehörig åtkomst, fastställa vilka handlingar som skall vara arkivhandlingar, verkställa gallring, m.m.[56]

När traditionella rutiner överförs till system för elektronisk dokumenthantering måste arkiveringsrutinerna uppmärksammas redan på planeringsstadiet. Det gäller såväl avställning av egentliga register som bildande av elektroniska akter. Se vidare om elektroniska akter m.m. i *bilaga 6*. Även gallringsfrågorna kommer normalt att aktualiseras i ett mycket tidigt skede om myndigheten planerar rutiner för scanning m.m.

[55] Se 11 § DL och 7 kap. 16 § sekretesslagen (1980:100).

[56] Verkställighetsföreskrifter utfärdas av Riksarkivet. De regler som rör IT-området återfinns främst i Riksarkivets regler om ADB-upptagningar (RA-FS 1994:2 och 1994:7). För närvarande pågår arbete med föreskrifter och allmänna råd om ärendeanknutna handlingar.

Myndigheterna får, enligt 10 § arkivlagen gallra allmänna handlingar. Vid gallring skall beaktas bl.a. att det arkivmaterial som återstår skall kunna tillgodose allmänhetens rätt att ta del av allmänna handlingar samt behovet av information för rättskipningen, förvaltningen och forskningen. Statliga myndigheter får, i enlighet med 14 § arkivförordningen, endast gallra allmänna handlingar med stöd av föreskrifter eller beslut från Riksarkivet, om inte särskilda föreskrifter om gallring har meddelats i lag eller förordning eller med stöd av 6, 6 a eller 18 § DL. För kommunerna får kommunfullmäktige respektive landstingsfullmäktige, i enlighet med 16 § arkivlagen, utfärda gallringsföreskrifter i den utsträckning annat inte är föreskrivet.

Som gallring räknas, enligt Riksarkivets föreskrifter, förstöring av allmänna handlingar och uppgifter i allmänna handlingar. Detta gäller även om handlingarnas innehåll dessförinnan överförts till annan databärare, om överföringen har inneburit informationsförlust, förlust av möjliga informationssammanställningar, förlust av möjligheter att fastställa informationens autenticitet eller förlust av sökmöjligheter. All överföring som medför informationsförluster för användaren ses alltså som gallring, även om det endast rör sig om "partiell gallring".[57]

Riksarkivets regler innebär exempelvis att det krävs särskilda gallringsföreskrifter för förstöring av de ursprungliga handlingarna såväl vid scanning av underskrivna pappershandlingar, som vid utskrift på papper av digitala dokument. Därtill kommer att överföringarna måste ske på det sätt som Riksarkivet föreskriver.

I ett antal lagar som reglerar register och aktmaterial där integritetsaspekterna är framträdande, har det tagits in bestämmelser om bevarande och gallring. Av dessa lagar är datalagen mest generell i sin räckvidd.

Utanför myndighetsområdet finns det inte några allmänna bestämmelser om arkiv. Datalagen gäller dock även för enskildas arkiv. I vissa andra författningar, som främst gäller ekonomiska förhållanden, finns bestämmelser om att handlingar skall bevaras under en bestämd tid. Som exempel kan nämnas lagen (1990:325) om självdeklaration och kontrolluppgifter.

Eftersom nuvarande regler om bevarande och gallring inte hindrar en övergång till elektronisk dokumenthantering lägger jag inte fram några författningsförslag i denna del. Myndigheter som överväger en övergång till sådana rutiner behöver emellertid på ett tidigt stadium observera de krav som följer av arkivförfattningarna; se vidare om arkiv, bevarande och gallring i *bilaga 3*. Det torde ofta vara lämpligt

[57] Utgångspunkten för Riksarkivets tolkning av gallringsbegreppet har varit användarnas behov av tillgång till allmänna handlingar med bibehållen kvalitet.

att myndigheten samråder med sin arkivmyndighet (6 § arkivförordningen).

6.5 Konsekvenser av mina förslag

Mina förslag syftar inte till nya åtaganden för det allmänna och det bör, som redan framgått, ges möjligheter men inte vara en skyldighet för enskilda att lämna eller ta emot uppgifter elektroniskt. Rätt tillämpade skall förslagen i stället ge förutsättningar för att med bibehållen rättssäkerhet rationalisera förvaltningen och förenkla uppgiftslämnandet.

Det är inte möjligt för mig att bedöma i vilken utsträckning olika myndigheter bör utnyttja de möjligheter som den nya tekniken och de föreslagna nya reglerna ger. Det får förutsättas att varje myndighet, liksom enskilda ingivare, väljer den mest rationella lösningen, och mindre myndigheter och ingivare kan behöva pröva i vilken omfattning ADB-stöd över huvud taget kan antas innebära någon rationaliseringsvinst.

Avdelning II
Elektronisk dokumenthantering inom näringslivet

7 Bakgrund

För några år sedan sågs de begränsningar som förelåg i datorernas kapacitet och i datorprogrammens funktioner som avgörande för valet av rutiner vid en övergång till IT. Fråga var om relativt begränsade tillämpningar, knutna till slutna miljöer och inriktade på att transaktioner registrerades och bearbetades klumpvis med vissa mellanrum. De funktioner som var betydelsefulla från civilrättsliga utgångspunkter kom därmed att utformas utifrån de tekniska förutsättningarna och avvikelserna från vedertagna synsätt blev i vissa fall betydande. Kraven på ökad effektivitet och behovet av snabba rationaliseringar förde därvid med sig att informationssystem togs i drift trots att rättsfrågorna inte hade klarats ut.

Den tekniska utvecklingen har nu gått dithän att datorernas kapacitet och möjligheterna till datakommunikation ger utrymme för att — inom acceptabla kostnadsramar och med bibehållen säkerhet — bryta ned hela handelsmönster till digitala operationer och att sekundsnabbt transportera data via nät. Rutinerna kan också, som framgått i den förvaltningsrättsliga delen, göras förenliga med de traditionella utgångspunkterna för rättssäker uppgiftshantering bl.a. genom en övergång till elektroniska dokument (med digitala signaturer eller stämplar) och överenskommelser mellan parterna om bl.a. det tekniska förfarandet.

De ökade kraven på effektivitet och konkurrensförmåga för emellertid med sig att övergången till IT, i stället för att begränsas till en omvandling av traditionella rutiner till motsvarande elektroniska förfaringssätt, ofta förenas med förändringar av hela handelsmönster. Som exempel kan nämnas koncepten "Just in Time" och "Business Process Reengineering", där även sådana krav som har uppfattats som självklara från rättsliga utgångspunkter kan bli ifrågasatta. — Exempelvis tar förändringsarbetet ofta sikte på automatiska *processer* och vissa ändamål som de är ämnade för, i stället för *produkter* såsom anbud, avtal, fakturor, leveranssedlar, etc. Strävanden att ta till vara hela den rationaliseringspotential som IT erbjuder har här lett till avvägningar mellan effektivitet och rättssäkerhet som i vissa fall kan behöva omprövas.

8 Avtalsrättsliga frågor

8.1 Utgångspunkter

Den civilrättsliga regleringen har i centrala delar kommit till inom ramen för nordiskt samarbete. Bestämmelserna är väl genomarbetade och de tillämpas i vissa delar analogt, utanför sitt egentliga tillämpningsområde, eller uppfattas som rättsgrundsatser. Det krävs därför starka skäl för ingrepp i denna reglering. Frågan är då hur den avtalsrättsliga regleringen kan tillämpas i IT-miljön.

Av 1 § första stycket avtalslagen (AvtL) framgår att avtal kommer till stånd genom anbud och svar som överensstämmer. I lagmotiven görs den påbyggnaden att avtal sluts genom utbyte av samstämmiga viljeförklaringar.[1] Avtalslagen är dock allmänt hållen och begränsad till allmänna principer som är tillämpliga på överenskommelser av skiftande slag. Den är inte uttömmande utan fragmentarisk[2] och parterna kan avtala om nya sätt att förplikta sig, samtidigt som en extensiv eller analog rättstillämpning är möjlig på området. Läran om avtals ingående, så som den har utvecklats i doktrin och praxis, uppvisar också en betydligt brokigare bild än den ganska enhetliga man får intrycket av vid läsningen enbart av avtalslagen och dess motiv. Lagtexten utesluter inte heller en anpassning till de olika förutsättningar som framträder inom skilda områden.

Det har emellertid inte gått att förutse alla sätt på vilka parter kan sluta avtal, och vissa gränser för möjligheterna till anpassning genom tolkning kan framträda när avtalslagen skall tillämpas på fakta som är helt annorlunda än de lagstiftaren har utgått från. Vid avtalslagens tillkomst fanns naturligtvis inte en tanke på att t.ex. datorer och elektronisk generering och förmedling av uppgifter skulle kunna ersätta traditionella skriftliga förfaranden, och användningen av IT i anknytning till nya handelsmönster medför ändrade förutsättningar för de rättsliga bedömningarna. Som kommer att framgå nedan torde de rättsfrågor som härvid aktualiseras i huvudsak kunna lösas genom avtal, men avtalslagen upptar också bestämmelser som inte kan avtalas bort,

[1] Förslag till lag om avtal etc., 1914, s. 36 och 49.

[2] Hellner, Jan, Lagstiftning inom förmögenhetsrätten, 1990, s. 89.

och tvingande regler ingriper mot alla förklaringar, även de elektroniska.

De avtalsrättsliga frågorna kan diskuteras utifrån ett par olika typfall.

I ett typfall utväxlar parterna anbud och accept osv. på sedvanligt sätt med medverkan av människor i varje led, och skillnaden i jämförelse med traditionell hantering är bara att meddelandena utväxlas på elektronisk väg. Tillämpningar av detta slag ger från rättslig synpunkt bara upphov till ganska begränsade frågeställningar.

I ett annat typfall kommer parterna, genom ett avtal om hur framtida avtal skall slutas, överens om hur anbud och svar m.m. skall kommuniceras automatiskt eller om hur varor successivt och automatiskt skall levereras och betalas inom ramen för ett avtal om långvarigt samarbete. Det blir alltså i detta typfall fråga om att tolka och tillämpa både den ursprungliga överenskommelsen och de senare avtal som ingås automatiskt med stöd av denna överenskommelse. Den ursprungliga överenskommelsen brukar betecknas EDI-avtal.[3] Där upptas även andra frågor som kan röra skilda rättsområden. Omfattande internationellt arbete har bedrivits för att utforma standardavtal på området.

Det finns emellertid också tillämpningar där parter sluter avtal utan att dessförinnan ha ingått avtal om förfarandet och där den ena parten — eller ibland t.o.m. båda — ändå använder sig av automatiska IT-rutiner. Den snabba spridningen av elektroniska rutiner för handel och administration för med sig krav på fungerande rättsliga förutsättningar för att sluta avtal även när parterna inte först har avtalat om det elektroniska förfarandet m.m.

Det har diskuterats om ett avtal måste grundas på en sådan samvilja som bara kan uppkomma när fysiska personer tar del av varandras viljeförklaring. Frågan är alltså om avtal över huvud taget kan slutas genom datorer utan direkt mänsklig inblandning och hur, i så fall, ett sådant avtalsslutande skall inordnas i det rättsliga systemet.

Enligt ett synsätt skulle det avtalsgrundande momentet falla tillbaka på en (hypotetisk) vilja hos den part som svarar för en helt automatisk rutin. Tanken är att de förklaringar som avges automatiskt får ses som avgivna av den person som har låtit installera och sätta i funktion en dator med programvaror för att ersätta fysiska personers viljeakter. Ett sådant synsätt kan vara träffande beträffande vissa av de meddelanden som utbyts i en sådan process. Helt automatiska EDI-rutiner är emellertid så sammansatta och komplicerade, samt i sådan grad påverkade av uppgifter som kommer från andra handelsparter, att det blir krystat att beskriva alla sådana förklaringar som ett inprogrammerat mekaniskt återgivande av en vilja hos systemets innehavare.

Enligt ett annat synsätt skulle ett informationssystem kunna ses som ett slags tredje man, varvid bestämmelserna om fullmakt skulle kunna tillämpas analogiskt. Någon tredje part med rättssubjektivitet är dock inte inblandad.

När den traditionella synen på hur avtal ingås skall föras ned på IT-miljöns praktiska plan framträder alltså vissa "störningar" i tänkesätt som brukar uppfattas som säkra utgångspunkter för juridisk argumentation.[4] De berörda tolkningarna visar vidare att ordens och de traditionella synsättens makt över tanken lätt kan underskattas.

[3] EDI = Electronic Data Interchange. — I mindre avancerade fall rör de meddelanden som successivt utväxlas kanske bara t.ex. leverans och betalning av varor i enlighet med EDI-avtalet, och processen innebär inte att det ingås några nya avtal.

[4] Jfr Grönfors, Kurt, Avtalsgrundande rättsfakta, 1993, s. 9 f.

8.2 Behovet av översyn

Ett delvis förändrat synsätt inom avtalsrätten är en ofrånkomlig följd av de nya IT-rutinerna. Det är varken ekonomiskt eller praktiskt försvarbart att söka framtvinga en imitation av traditionella handelsmönster när det — utan att åsidosätta andra skyddsintressen — blir möjligt att införa effektivare och säkrare rutiner. Min utgångspunkt är därför att de rättsverkningar som parter avser att uppnå bör kunna inträda också med användning av elektroniska rutiner.

Det bör härvid undvikas att frågan om elektroniska avtalsslut reduceras till en bedömning av om de begrepp som avtalslagen bygger på kan tolkas så att en (endast) maskinell "vilja" kan läggas till grund för ett avtal. I stället bör de bakomliggande behoven av rättsligt skydd för de praktiska tillämpningarna lyftas fram. Såväl företagen som myndigheter och privatpersoner behöver kunna dra nytta av de nya rutinerna på ett effektivt och rättssäkert sätt.

Användningen av EDI så att förklaringar genereras automatiskt är regelmässigt begränsad till transaktioner som är vanligt förekommande. En motsvarighet i traditionell miljö utgör de s.k. *massavtalen*, som ingås i stor mängd i det dagliga livet. Typiskt för denna grupp av avtal är upprepningen av ett enkelt mönster såsom enkla inköp till små belopp i butik eller en bussfärd mot kontant betalning. Massavtal kräver särregler[5] och uttunnade former för avtalsslut eller att avtalsslut genom faktiskt handlande godtas.[6]

Som ett exempel kan nämnas att avtal om parkering anses uppkomma genom den faktiska åtgärden att ställa upp bilen på parkeringsplatsen. Ett annat exempel är det köpeavtal som uppkommer när någon matar in pengar i en varuautomat. På motsvarande sätt bör det rättssubjekt som elektroniskt och med automatik avger ett anbud eller en accept uppenbarligen bli bunden av anbudet eller svaret. Hela förfaringssättet syftar ju till bindande överenskommelser.[7]

I stället för att laborera med en hypotetisk eller fingerad viljeförklaring där klara viljeelement saknas, uppkommer avtalsbundenhet som ett slags sanktion, till följd av vissa yttre omständigheter som kombinerade med varandra fungerar som direkt avtalsgrundande.[8] Fråga är om

[5] NJA 1992 s. 267.

[6] Jfr Bernitz, Standardavtalsrätt, 6 u., s. 33.

[7] De tekniska och administrativa rutinerna får emellertid inte missförstås, t.ex. så att en bekräftelse av ett anbud, i syfte att säkerställa att meddelandet kommit fram, felaktigt uppfattas som en "accept".

[8] I vissa fall har rättspolitiskt önskvärda bedömningar åstadkommits genom anpassningar av mekanismen för avtals ingående så att ett avtal anses föreligga. Som exempel på tidiga sådana konstruktioner kan nämnas tysta viljeförklaringar eller förklaringar i form av konkludent handlande, medan senare exempel visat en tendens att grunda avtalsverkan direkt på vissa rättsfakta, utan en omväg via en (konstruerad) samvilja. I andra fall har rättspolitiskt motiverade förskjutningar mellan tillämpningsområdet för bestämmelser som

situationer där de praktiska behoven har framtvingat avtalsverkningar, trots att en viljeförklaring i traditionell mening inte längre föreligger.[9] Lagtexten är tillräckligt rymlig för att tillåta en sådan fortsatt objektivering av avtalsrätten, samtidigt som nya och från civilrätten i övrigt avvikande rättsliga konstruktioner kan undvikas.

Som kommer att framgå närmare nedan, torde avtalslagen också i huvudsak kunna tillämpas på de rättsfrågor som härvid aktualiseras. Exempelvis är reglerna om avtals giltighet och tolkning i princip inte beroende av sättet för kommunikation (jfr dock nedan angående 32 § AvtL), och de moment av direkt mänsklig vilja som i vissa fall saknas i anknytning till IT, synes i huvudsak inte utesluta en fungerande tillämpning av gällande rätt vid prövningen av frågor om avtals ingående och innebörd. Den avtalsrättsliga regleringen behöver därför inte bli föremål för några genomgripande ändringar, och sådana frågor som inte direkt faller in under någon gällande bestämmelse bör ändå kunna lösas i nära anslutning till de principer på vilka avtalslagen grundas.

Den osäkerhet som på IT-området kan framträda rörande vissa detaljfrågor bör alltså inte föranleda någon särreglering inom avtalsrätten. Ännu mindre bör det införas någon detaljreglering för rutiner baserade på nya handelsmönster. De omfattande regler som skulle bli följden av ett sådant tillvägagångssätt skulle — på grund av den intensiva utvecklingen inom området — med all säkerhet inte få den stabilitet och varaktighet som bör kännetecknа den centrala civilrätten.

I det följande tar jag upp olika praktiska frågor om tillämpningen av avtalslagen i IT-sammanhang. Det gäller frågor om rättsverkningar av avsändande och mottagande av elektroniska meddelanden (avsnitt 8.3.1 — 8.3.3), om tillämpningen av regler som kräver mänskliga förhållningssätt (avsnitt 8.3.4) samt om risken för förvanskning vid överföring av meddelanden (avsnitt 8.3.5). I sistnämnda del föreslår jag en ändring i avtalslagen.

I *bilaga 4* behandlas det behov som finns av modellösningar, för att handelsparter enklare skall kunna förutse hur berörda rättsfrågor är att bedöma.[10]

gäller inom respektive utom kontrakt åstadkommits så att avtalsverkan anses inträda utan att ett avtal anses föreligga, se vidare Grönfors, a.a., s. 97 f.

[9] Grönfors, a.a. s. 55.

[10] Bilagan är visserligen inriktad på förvaltningsmyndigheternas ärendehandläggning, men det är samma behov av anpassningar som aktualiseras.

8.3 Att sända och motta förklaringar

8.3.1 Rättsverkningar genom avsändande

Inom avtalsrätten inträder i vissa fall rättsverkningar redan genom att en förklaring *avsänds*. Enligt 40 § första stycket avtalslagen (AvtL) går vissa meddelanden på mottagarens risk; det är fråga om sådana situationer där skyldigheten att lämna ett meddelande är stadgad i mottagarens intresse.[11] Härvid krävs endast att meddelandet har inlämnats för befordran med post eller telegraf eller eljest har avsänts "på ändamålsenligt sätt".

I IT-miljön aktualiseras frågan om elektronisk befordran innebär att meddelandet har lämnats för befordran på ändamålsenligt sätt och — om så är fallet — hur man bör bestämma vid vilken tidpunkt ett sådant meddelande har avsänts.[12] Här kan närmast tekniska resonemang aktualiseras. Hur pålitligt är systemet och är meddelandet avsänt redan när informationssystemet har mottagit en instruktion om att sända meddelandet?

Bestämmelsen i 40 § första stycket AvtL överensstämmer med motsvarande regel i 61 § i 1905 års köplag. Almén har i sin kommentar till köplagen, med hänvisning till lagmotiven, anfört att befordran med post eller telegraf är de enda ändamålsenliga sätten att genom annan sända meddelanden mellan orter som har post- eller telegrafförbindelse med varandra, eller inom orter där lokalpost är anordnad.[13] Detta synsätt är uppenbarligen föråldrat. Inom affärslivet är det sedan många år allmänt accepterat att kommunicera via telex och telefax.[14] E-post och liknande rutiner för elektronisk kommunikation börjar nu också bli vedertagna. Bestämmelsen i 61 § i 1905 års köplag motsvaras av 82 § i 1990 års köplag, där det endast sägs att aktuella meddelanden skall ha "avsänts på ett ändamålsenligt sätt".[15] Regleringen i avtalslagen bör uppenbarligen förstås på samma sätt, dvs. att 40 § blir tillämplig när ett meddelande har avsänts på ett sätt som är ändamålsenligt med hänsyn till den föreliggande situationen.

När parterna har använt t.ex. e-post för att kommunicera anbud och accept är det naturligtvis ändamålsenligt att sända även ett sådant

[11] Se 4, 6, 9, 19, 28 och 32 §§ AvtL.

[12] Jfr de ovan berörda standardiserade rutinerna för informationssäkerhet där bevis om avsändande, om fullbordad förmedling och om mottagande kan genereras.

[13] Almén/Eklund, Om köp och byte av lös egendom, 1960, s. 805, där det också sägs att en reklamationsskyldig som anlitar ett stadsbud i stället för posten, själv synes böra stå risken för att meddelandet inte kommer adressaten till handa, en regel som enligt Almén skulle gälla åtminstone om meddelandet skickats med en anställd hos avsändaren.

[14] Att telefaxmeddelanden ofta bekräftas genom vanligt brev för att säkra bevisning bör inte föranleda någon annan bedömning.

[15] Prop. 1988/89:76 s. 217 och NU 1984:5 s. 377 f.

meddelande som avses i 40 § AvtL på detta sätt.[16] På IT-området aktualiseras emellertid en mängd skilda situationer. När parterna brukar översända sin affärskorrespondens så att avsändaren automatiskt får en kvittens på att meddelandet har nått mottagarens elektroniska adress[17] kan det ifrågasättas om samma krav på säkerhet bör ställas för att ett meddelande enligt 40 § AvtL skall anses ha avsänts på ett ändamålsenligt sätt.[18] Det kan också vara så att en part som inte tidigare har kommunicerat elektroniskt med sin motpart, elektroniskt översänder ett meddelande som avses i 40 § AvtL, varefter motparten hävdar att det inte varit försvarligt med hänsyn till den föreliggande situationen att reklamera elektroniskt.

Vanligtvis bör det enligt min bedömning inte råda någon tvekan om att parter som brukar överbringa affärskorrespondens elektroniskt kan använda sådan kommunikation också för de meddelanden som avses i 40 § AvtL. Dessa frågor bör emellertid lösas i praxis, och det bör beaktas att även andra faktorer än meddelandets form kan ha betydelse för denna bedömning, t.ex. frågan om hur brådskande åtgärden har varit.

Beträffande frågan *när* en elektronisk handling anses ha avsänts bör ett praktiskt synsätt vara möjligt inom ramen för gällande rätt. När avsändaren har lagt ett brev på brevlådan eller beställt ett telegram har han fullgjort allt som på honom ankommer för att försändelsen skall överbringas till adressaten. En naturlig tolkning av gällande rätt är härvid att ett elektroniskt meddelande anses avsänt när avsändaren har gett sitt meddelandesystem de instruktioner som behövs för att sända meddelandet och fått kvittens på att instruktionerna är accepterade.[19]

I detta sammanhang aktualiseras också andra praktiska frågor, t.ex. hur avsändaren skall kunna veta att en reklamation sänds till rätt adress när mottagaren inte har uppgivit viss elektronisk adress och det saknas tillförlitliga kataloger över sådana elektroniska adresser.[20] Det är varken

[16] Parter som kommunicerar med strukturerade meddelanden (EDI), där hela förfarandet har automatiserats, bör kunna bruka de vedertagna kommunikationsvägarna även för reklamationer, under förutsättning att IT-rutinerna kan hantera även reklamationer. Detta är praktiskt möjligt endast om det finns standardiserade meddelanden för reklamation och programvarorna kan hantera sådana rutiner.

[17] Ang. detta begrepp, se avsnitt 3.3.2 och bilaga 5.

[18] Härvid avses inte att risken för att elektroniska meddelanden försenas eller kommer bort skall övervältras på avsändaren utan att det kan ifrågasättas om valet av kommunikationsform kan anses ändamålsenligt. Bestämmelsens avfattning utesluter inte att avsändaren kan bli skyldig att sända ett nytt meddelande om han får veta att det föregående har förkommit (NJA II 1915 s. 289).

[19] Jfr avsnitt 3.3.2 rörande inkommande handlingar, där mitt synsätt inte har knutits till fysiska platser utan elektroniska adresser.

[20] Jfr de komplikationer som berörs i bilaga 5 angående gränsdragningen mellan privata elektroniska adresser resp. adresser som används i arbetet.

möjligt eller lämpligt att detaljreglera dessa frågor i lag. De bör i stället, som i dag, lösas i praxis.

8.3.2 Rättsverkningar genom mottagande

I andra sammanhang är det avgörande när en förklaring *kommit till handa*.[21] Därvid krävs inte att mottagaren verkligen har tagit del av meddelandet. Avgörande är om mottagaren har beretts tillfälle att ta del av innehållet. Mottagaren bär från denna tidpunkt risken för bristande kunskap om meddelandets innehåll. Ett annat synsätt skulle medföra orimliga beviskrav för avsändaren. Parterna kan dock vanligtvis genom avtal reglera under vilka förutsättningar en förklaring skall anses få rättsverkningar.

När det i avtalslagen anges att ett meddelande skall ha kommit någon "till handa" är huvudtanken den att mottagaren faktiskt skall ha satts i tillfälle att omedelbart ta del av meddelandets innehåll. Med utgångspunkt häri får man pröva vad som krävs för att ett meddelande i det särskilda fallet skall anses ha kommit adressaten till handa när t.ex. e-post eller telefax används.[22] Härvid aktualiseras motsvarande bedömningar som för inkommande elektroniska handlingar enligt RB, FPL och FL.

Ett elektroniskt meddelande som har överförts till den funktion i adressatens informationssystem där meddelanden tas emot bör anses ha kommit denne till handa (mottagarens elektroniska adress); jfr traditionell post som har befordrats till adressatens kontor. Om adressaten i stället har en elektronisk brevlåda hos ett företag som tillhandahåller sådana tjänster, bör meddelandet vanligtvis anses ha kommit adressaten till handa redan när det har nått denna brevlåda, dvs. det elektroniska "utrymme"/den funktion hos befordringsföretaget där inkommande elektroniska handlingar förvaras för adressatens räkning.[23] Visserligen skall meddelandena gå på avsändarens risk när det föreskrivs att de skall ha "kommit till handa" — det är i dennes intresse som meddelandet har avsänts[24] — men det är inte rimligt att avsändarens rätt skall bli beroende av vid vilken tidpunkt adressaten "hämtar" sin e-post; jfr vanlig post som sorterats in i adressatens postbox.[25] Skulle elektroniska "utrymmen" där elektroniska handlingar mottas, i detta avseende,

[21] Se t.ex. 2, 3 och 7 §§ AvtL.

[22] Grönfors, Avtalslagen, 3 u., s. 71.

[23] Med ett sådant synsätt är det möjligt att hantera också sådan kommunikation där en av parterna tillhandahåller t.ex. en elektronisk brevlåda åt motparten.

[24] Grönfors, a.a., s. 79.

[25] Dröjsmål med att avhämta traditionell post som har sorterats in i adressatens postbox för ankommande försändelser torde vanligtvis inte få åberopas av adressaten (Grönfors, a.a., s. 71).

behandlas olika när de är knutna direkt till adressatens informationssystem respektive till ett företag som tillhandahåller sådana "postboxar", kunde de som sänder elektroniska meddelanden bli ställda inför närmast slumpmässiga variationer, eftersom de ofta torde sakna möjlighet att av t.ex. adresseringen utläsa om en överföring till en viss elektronisk adress innebär att meddelandet kommer att lagras av någon annan i avvaktan på en åtgärd från adressaten.

Valet av kommunikationsväg aktualiserar också frågan om meddelandet skall anses ha kommit adressaten till handa så snart det är *tekniskt möjligt* för adressaten att "hämta" meddelandet, oavsett till vilken elektronisk adress meddelandet har sänts; jfr de frågor som har tagits upp i anknytning till bestämmelserna i 2 kap. TF och 40 § AvtL.[26]

Tidigare har i huvudsak endast kommunikation via traditionell post, telegram eller telex varit aktuell, och dessa kommunikationsformer har varit begränsade till antalet och har kringgärdats med sådana rutiner för att ta hand om och ta del av försändelser att det är naturligt att adressaten får stå risken om han inte vidtar de åtgärder som behövs för att han skall få del av meddelandenas innehåll.[27] Utvecklingen av nät för datorkommunikation och av olika tjänster för bl.a. förmedling av meddelanden har emellertid fört med sig att flitiga användare av IT vanligtvis tilldelas en mängd olika elektroniska adresser.[28] Detta kan ske genom att användaren t.ex. anmäler sig till en viss elektronisk tjänst via vilken det samtidigt tillhandahålls en funktion för e-post, trots att användaren inte är intresserad av den funktionen.[29]

För att en handling som överförts elektroniskt skall anses ha kommit adressaten till handa bör det krävas att det är fråga om en elektronisk adress som adressaten verkligen använder eller har angivit att han använder.[30] Detta krav får anses ligga i uttrycket att meddelandet skall ha kommit adressaten "till handa".

Dessa frågor bör alltså kunna lösas i praxis, utifrån i huvudsak samma utgångspunkter som för traditionell kommunikation.

[26] Dvs. regler som gäller när annan har gjort en upptagning tillgänglig för en myndighet så att upptagningen är att anse som inkommen resp. när en handling har inlämnats för befordran på ändamålsenligt sätt.

[27] Han får själv stå risken om han inte hämtar sin post eller läser de telexmeddelanden som tas emot med hans tekniska hjälpmedel.

[28] En renodlad utgångspunkt från adressatens tekniska möjligheter att överföra en elektronisk handling till läsbar form skulle kunna leda till att en handling anses ha kommit adressaten till handa trots att han inte rimligen kan förväntas känna till dess existens, t.ex. när handlingen har sänts till en elektronisk anslagstavla där adressaten sällan loggar in.

[29] Jfr avsnitt 3.3.3.

[30] Den elektroniska adressen kan ha angivits av adressaten på dennes brevpapper eller liknande material eller i kataloger där företagets elektroniska adress anges. Här aktualiseras samma behov av ordning och reda som berörts i den processuella delen.

I ett avseende skiljer sig den civilrättsliga regleringen dock från huvudregeln enligt de processuella reglerna om inkommande handlingar. Enligt den processuella regleringen är det tillräckligt att handlingen har överbringats kl. 24 en viss dag för att den skall anses ha kommit in den dagen. Den civilrättsliga regleringen innebär emellertid att ett brev eller ett telegram, som har ankommit till mottagaren utom den på platsen och inom branschen sedvanliga kontorstiden, anses komma adressaten till handa först följande arbetsdags morgon, såvida inte adressaten dessförinnan faktiskt har tagit del av handlingens innehåll.[31] Detta synsätt bör kunna tillämpas också i IT-miljön. De nya rutinerna kan emellertid komma att påverka vad som bör ses som kontorstid.[32]

Vid elektronisk kommunikation kan tekniska fel, bristande kompatibilitet, kryptering, komprimering m.fl. hinder medföra att data visserligen kommer adressaten till handa men att denne inte alls eller först senare kan läsa meddelandet.[33] När det är fråga om meddelanden som befordras i avsändarens intresse bör denne stå risken också för att meddelandet inte kan läsas av mottagaren. Meddelandet bör alltså i princip anses ha kommit till handa först när det kan göras läsbart av mottagaren. Adressaten bör emellertid inte kunna undandra sig rättsverkningar genom att förfoga över denna tidpunkt så att han utan skäl och utan att meddela därom gör sig ur stånd att kommunicera på de sätt hans affärskontakter tidigare har använt eller som han annars har gett sin omgivning anledning att förvänta. Även denna fråga bör kunna lösas i praxis. Den fortsatta utvecklingen av elektronisk kommunikation torde dock komma att begränsa riskerna för sådana komplikationer genom att meddelandeformat m.m. standardiseras och att det införs tekniska kontrollrutiner såsom kvittenser på att meddelanden har nått en viss elektronisk adress.

[31] Grönfors, a.a., s. 71.

[32] Som exempel kan nämnas att automatiskt genererade och överförda strukturerade meddelanden, s.k. Electronic Data Interchange (EDI), som avses hanteras och besvaras endast maskinellt, kan antas komma att behandlas av parternas informationssystem oberoende av när under dygnet meddelandet når fram. Vidare tenderar de elektroniska kommunikationsformernas snabbhet och internationalisering att leda till frister i timmar och minuter i stället för dagar och till i det närmaste omedelbara överföringar av meddelanden mellan skilda tidszoner.

[33] Jfr regleringen av inkommande handlingar enligt RB, FPL och FL, där jag av praktiska skäl har föreslagit en regel som innebär att en handling anses inkommen när data har nått adressaten men att handlingar som myndigheten inte kan läsa får behandlas på motsvarande sätt som en traditionell skrift som är avfattad på ett språk som myndigheten inte behärskar, se vidare avsnitt 3.4.

8.3.3 Frister vid skriftlig respektive muntlig kommunikation

I IT-miljön kan det vid beräkning av en acceptfrist bli betydelsefullt huruvida elektronisk kommunikation bör ses som muntlig eller som brev/telegram, dels när anbudsgivaren inte har satt ut någon tid för svar (3 § AvtL), dels när viss tidsrymd för svar har satts ut och det skall avgöras från vilken tidpunkt fristen löper (2 § andra stycket AvtL). — Det finns knappast något enkelt och generellt svar. IT-rutiner kan användas på vitt skilda sätt; jfr att Internet kan användas för såväl elektronisk post som samtal i realtid.

Bland de skillnader som framträder mellan muntlig respektive skriftlig kommunikation kan nämnas att parter som kommunicerar skriftligen koncentrerar och tydliggör sina förklaringar i högre grad än vid muntlig kommunikation och att det vid skriftlig kommunikation vanligtvis är enklare att skilja preliminära överläggningar från bindande förklaringar.

För de här aktuella tolkningsreglerna är emellertid tidsaspekten det centrala. Eftersom samma elektroniska kommunikationsleder vanligtvis kan användas både för tal, text och bild — i realtid eller utan direkt kontakt mellan parterna — bör bedömningen falla tillbaka på IT-användningen i det enskilda fallet. Att bestämmelsen i 2 § andra stycket AvtL inte innehåller någon regel för muntlig kommunikation beror uppenbarligen på att saken varit självklar för de fall där parterna samtalar. Om den som ger ett anbud anger en tidsrymd inom vilken svar skall komma honom till handa, löper fristen naturligtvis från samtalstillfället. Härvid torde det sakna betydelse om parterna talar respektive lyssnar på vad den andre säger eller om de är direkt uppkopplade så att de skriver text till varandra som omedelbart visas på den andres bildskärm. Det avgörande är om kommunikationen sker direkt eller indirekt. Uttalandena i lagmotiven bör — tolkade från nu angivna utgångspunkter — kunna bilda utgångspunkt för bedömningen av regelns användning också på IT-området.[34] Detsamma gäller vad som bör vara att anse som skriftlig respektive muntlig kommunikation enligt 3 § AvtL.[35]

I dessa bestämmelser framträder också skillnader mellan brev och telegram, dels eftersom telegram innehållsmässigt hanteras av en tredje part (2 § andra stycket), dels eftersom telegram befordras snabbare än

[34] Grönfors, a.a., s. 72 och 74.

[35] Nuvarande utveckling mot att olika medier och former för kommunikation integreras så att gränserna delvis suddas ut kan dock antas föra med sig tolkningssvårigheter, och det bör noteras att en del av de funktioner som e-post har hämtat från vanlig post har försvagats. Som exempel kan nämnas att e-posten ofta inte läses och annars hanteras så noggrant som vanlig post.

vanlig post (3 § första stycket). Regleringen har inskränkts till brev och telegram (jämte muntliga anbud) därför att övriga metoder vid lagens tillkomst var relativt sällsynta och oviktiga.[36] Enligt min mening bör regleringen i denna del förstås så att rutiner inom ramen för s.k. tredjepartstjänster[37] jämställs med telegram. En tidsstämpling av en tredje part vid "skriftlig" kommunikation bör alltså tas till utgångspunkt för en beräkning av tid enligt 2 § andra stycket AvtL. Vidare bör en anbudsgivare som använder snabb elektronisk kommunikation — jfr anbud genom telegram — kunna förutsätta att svaret kommer honom lika tidigt till handa (3 § första stycket AvtL). Därmed torde det inte heller i denna del krävas några ändringar i lag.

8.3.4 Tillämpningen av vissa regler som kräver mänskliga förhållningssätt

Som framgått av föregående avsnitt kan åtgärder som har vidtagits helt automatiskt av datorer få rättsverkan. Frågan är då hur avtalsrättsliga regler som förutsätter en direkt inblandning av fysiska personer bör tolkas i detta nya sammanhang.

Enligt vissa bestämmelser är det avgörande om mottagaren verkligen har tagit del av ett meddelande eller äger vetskap om ett visst förhållande (se t.ex. 7 och 39 §§ AvtL). Kan sådan "vetskap" inträda inom ramen för helt eller delvis automatiska rutiner och när inträder den i så fall? På motsvarande sätt kan ifrågasättas om ond eller god tro kan föreligga (se t.ex. 4, 6 och 9 §§ AvtL) och om ogiltighetsreglerna i 3 kap. AvtL kan tillämpas vid helt automatiska rutiner. Kan t.ex. ett svikligt förledande enligt 30 § AvtL ske genom att en dator manipulerar en annan?

Samtidigt som lagstiftaren i avtalslagens motiv förde in vissa subjektiva moment såsom utgångspunkten från *vilje*förklaringar tar motiven avstånd från den i äldre rätt hyllade s.k. *viljeteorin*, dvs. att partens vilja med förklaringen blir avgörande för avtalsverkan. För att bereda skydd för affärslivet byggde lagstiftaren i stället på den s.k. *tillitsteorin*, vilken innebär att den tillit som förklaringen ger upphov till hos motparten anses leda till avtalsverkan. Nödvändigheten att kunna lita på avgivna förklaringar bildade således basen för avtalslagen och perspektivet försköts från avgivarens vilja med förklaringen till den tillit som förklaringen väckt hos medkontrahenten.[38]

Den fortsatta utvecklingen har fört med sig helt nya tekniska och administrativa rutiner samt till följd härav nya handelsmönster, där rutinerna för avtalsslut inte alltid kan sorteras in under den traditionella utgångspunkten från en parts vilja. Enligt en numera allt oftare hävdad

[36] Grönfors, a.a., s. 74.

[37] Sådana är under snabb utveckling, och tidsstämpling av meddelanden anses vara en funktion som bör skötas av en s.k. Trusted Third Party.

[38] Grönfors, Avtalsgrundande rättsfakta, 1993, s. 18.

teori, den s.k. *förklaringsteorin*, bör i stället själva förklaringen sättas i centrum så som den framträder för en objektiv betraktare.

Enligt min mening kan bedömningar utifrån subjektiva element, såsom en parts vilja, i princip inte göras när automatiska rutiner har ersatt manuella ställningstaganden.[39] Därmed kan bestämmelserna i 4 § andra stycket, 6 § andra stycket och 9 § andra meningen AvtL inte tillämpas på mellanhavanden som hanteras automatiskt. En sådan tillämpning skulle förutsätta bedömningar av vad avsändaren utgår från respektive vad mottagaren inser, trots att sådana mänskliga förhållningssätt inte föreligger vid helt automatiska rutiner.[40] Detta innebär alltså att t.ex. en försenad accept (i förening med passivitet från motpartens sida) i ett helt automatiserat system inte kan leda till något avtal. Detta torde emellertid knappast ha någon praktisk betydelse. Man kan räkna med att system av detta slag antingen accepterar det nya anbud som den försenade accepten innebär eller ger en signal till den som sköter systemet om att det har inträffat en situation som måste tas om hand av människor.

På motsvarande sätt bör 28-31 §§ AvtL om tvång, svek och ocker inte kunna tillämpas. En maskin kan inte tvingas eller svikligen förledas till att företa en rättshandling och en dator kan inte sägas vara i trångmål, oförståndig, lättsinnig eller i beroendeställning. Inte heller 33 § (tro och heder) kan komma till användning annat än under mycket speciella förhållanden. En annan sak är att ogiltighetsreglerna kan vara tillämpliga på EDI-avtalet, om det finns ett sådant.

Bestämmelsen i 32 § första stycket AvtL om förklaringsmisstag bör inte heller anses vara användbar vid en prövning rörande en automatiskt genererad förklaring. En tillämpning av bestämmelsen förutsätter att det "objektiva" förklaringsinnehållet först fastställs och att det därefter undersöks i vad mån detta innehåll avviker från det av avgivaren åsyftade. Löftesgivarens vilja skall alltså åtskiljas från förklaringen i övrigt. En sådan distinktion kan inte upprätthållas vid automatiskt genererade förklaringar, och stadgandet kan därmed inte tillämpas.[41] Vidare kan en prövning av om mottagaren har insett eller bort inse misstaget knappast ske när mottagaren är en dator som agerar auto-

[39] Att t.ex. äga vetskap, vara i ond tro eller vara vilseledd är förhållningssätt som, i vart fall språkligt, anses vara förbehållet människor. Härvid bör dock uppmärksammas att regleringen naturligtvis kan tillämpas på vanligt sätt när en fysisk person har varit inblandad i det enskilda fallet.

[40] Se Grönfors, Kurt, Avtalslagen, 3 u., s. 77.

[41] Grönfors, a.a., s. 197 och Vahlén, Avtal och tolkning, s. 31.

matiskt.[42] (Beträffande denna paragrafs tillämplighet på icke automatiserade elektroniska tillämpningar, se nästa avsnitt.)

Ogiltighetsreglerna i 28-33 §§ AvtL har dock minskat i betydelse i och med införandet av generalklausulen om oskäliga avtalsvillkor i 36 § AvtL,[43] och generalklausulens abstrakta utformning och avsaknad av subjektiva rekvisit gör den väl lämpad även för frågor som aktualiseras vid helt automatiska rutiner.

Enligt 7 § AvtL kan ett anbud eller en accept återkallas till dess mottagaren har tagit del av anbudet eller svaret. Bestämmelsen kompletteras av 39 § samma lag, enligt vilken återkallelse undantagsvis kan ske så länge rättshandlingen inte har inverkat bestämmande på mottagarens handlingssätt. Regleringen avser sådana praktiska omständigheter på vilka även helt automatiska EDI-rutiner bör kunna tillämpas. Har ett anbud kommit mottagaren till handa, t.ex. i hans elektroniska brevlåda[44], och avsändaren därefter sänder en återkallelse som når samma brevlåda innan mottagarens helautomatiska EDI-system har behandlat ("tagit del av") anbudet, bör bestämmelsen kunna tillämpas på motsvarande sätt som när en fysisk person vid ett visst tillfälle tar del av både ett anbud och en återkallelse.[45] Även 39 § AvtL bör kunna tillämpas på sådana fall. Att detta synsätt är motiverat framgår av att den berörda regleringen inte syftar till bedömningar av subjektiva förhållningssätt utan till att dra en gräns utifrån när ett meddelande så att säga har nått ända fram till adressaten eller i yttre mening har inverkat bestämmande på hans handlingssätt. — Det som nu har sagts om 7 och 39 §§ AvtL förutsätter dock att systemen är byggda så att återkallelsen kan stoppa verkställigheten av det första meddelandet. Det är alltså snarare EDI-avtalet än lagtexten som avgör om återkallelsen skall få någon effekt.[46]

[42] Här bör undvikas komplicerade teoretiska överbyggnader baserade på någon slags ursprunglig vilja som kommit till uttryck vid t.ex. programmering eller systemkonstruktion, kanske dokumenterad i systemdokumentationen. I stället aktualiseras behovet av en systempolicy som inte bara handlar om teknisk dokumentation utan också om systemets ändamål och de särskilda hänsyn som bör tas, med beaktande av olika typer av risker. När rimlighetskontroller etc. förutsätts och borde ha gett utslag kan i stället frågor om oaktsamhet aktualiseras.

[43] Grönfors, a.a., s. 206 f.

[44] Jfr avsnitt 8.3.2. Detsamma bör gälla om exemplet modifieras så att både anbudet och återkallelsen förvaras i adressatens informationssystem i avvaktan på att bli behandlade av systemets EDI-funktion.

[45] Vid automatiska EDI-rutiner kan det naturligtvis inte godtas att återkallelse sker ända till dess en fysisk person har tagit del av anbudet eller svaret. Ett sådant synsätt skulle kunna leda till en möjlighet att återkalla en förklaring trots att motpartens EDI-rutiner låtit t.ex. tillverka en beställd vara; jfr om köp av varor i en automat skulle kunna återkallas efter att kunden har lagt i pengarna och fått varan.

[46] Här bortses från att den part som är medveten om att hans meddelandesystem har avgett ett anbud oftast torde kunna återkalla anbudet enligt reglerna i 7 och 39 §§ AvtL genom ett särskilt meddelande direkt till motparten.

Enligt min mening krävs det alltså inte heller i denna del några ändringar i lag med anledning av en övergång till helt automatiska rutiner.

8.3.5 Särskilt om befordringsfel

En utgångspunkt inom avtalsrätten är att avsändaren står risken för att hans meddelande inte kommer fram i tid eller på rätt sätt.[47] Undantag gäller enligt 40 § AvtL för vissa typer av meddelanden, där skyldigheten att skicka meddelandet har föreskrivits i mottagarens intresse; om ett sådant meddelande har avsänts på ändamålsenligt sätt, står mottagaren risken för att meddelandet försenas eller inte kommer fram.[48] Dessa allmänna principer bör naturligtvis gälla också för meddelanden som befordras elektroniskt.

I 32 § AvtL finns bestämmelser för olika fall när en viljeförklaring får ett annat innehåll än det avsedda. Bestämmelserna gäller oavsett i vems intresse det ligger att meddelandet skickas. I första stycket behandlas förklaringsmisstag, dvs. felskrivningar och andra misstag varigenom en viljeförklaring får ett annat innehåll än avsett. Andra stycket handlar om vissa befordringsfel, närmare bestämt fel vid telegrafering och felaktigt muntligt framförande av ett bud. Medan regeln i första stycket skyddar mottagaren, skyddar regeln i andra stycket avsändaren.

Enligt Grönfors kommentar till avtalslagen[49] saknas grund för en analogisk tillämpning av bestämmelsen om befordringsfel på t.ex. telex, telefax och e-post, eftersom parterna då får anses komma i direkt kontakt med varandra utan att någon annan person, såsom telegrafisten eller budet, kommer emellan. Motsatt synsätt har förts fram särskilt i IT-rättsligt inriktade sammanhang,[50] där det har ifrågasatts om det finns sådana rättsligt relevanta skillnader mellan fel vid elektronisk kommunikation och befordran via telegraf att det är motiverat med skilda synsätt.[51]

[47] Prop. 1988/89:76 s. 217 och NU 1984:5 s. 378.

[48] Jfr Grönfors, a.a., s. 266.

[49] Grönfors, a.a., s. 202, se även Ramberg, J, Allmän avtalsrätt, 2 u., s. 193.

[50] Se t.ex. Einersen, E., Elektronisk aftale- & bevisret, 1992, s. 71 f.

[51] Som skäl för att regeln om befordringsfel bör gälla all elektronisk kommunikation har åberopats vissa gemensamma egenskaper hos telegrafi resp. telefax och annan elektronisk kommunikation. Härvid har nämnts bl.a. följande. Det är stor risk för fel vid såväl telegrafi som elektronisk kommunikation. Kontrollprocedurerna vid elektronisk kommunikation indikerar inte alla de fel som kan uppkomma och vanligtvis kan ingen av parterna lastas. Felen uppkommer ofta vid modemkontakter på ett allmänt tillgängligt telenät där nätoperatören har friskrivits från ansvar. Telegramregeln i 32 § AvtL har kommit till av samhällsekonomiska skäl, för att befordra användningen av denna kommunikationsform, och samma skäl kan åberopas på IT-området. Utvecklingen går mot alltmer avancerade tredjepartstjänster för konvertering, autenticering, hantering av nycklar

Rutiner och teknik för kommunikation inom affärslivet har nu förändrats så att telegram knappast förekommer.[52] I stället kommunicerar handelsparter med t.ex. telefax, EDI och e-post. Härvid kan parterna sägas få direkt kontakt på så sätt att en teleförbindelse upprättas mellan dem via vilken meddelandet distribueras direkt till adressatens tekniska utrustning. Det förekommer emellertid också ett flertal olika tjänster för elektronisk förmedling där en tredje part, ett befordringsföretag, tillhandahåller olika tjänster bl.a. för e-post.[53]

Det är enligt min mening uppenbart att 32 § första stycket AvtL inte kan tillämpas när ett elektroniskt meddelande, som vid avsändandet har det innehåll som avsändaren har avsett, blir förvanskat under överföringen till mottagaren.

En gränsdragning så att 32 § andra stycket AvtL skulle tillämpas om felet uppkommit vid manuella åtgärder hos ett befordringsföretag men inte när förvanskningen orsakats av maskinella fel torde, på grund av utredningssvårigheter, knappast kunna tillämpas i praktiken. En gränsdragning utifrån hur omfattande tjänster den tredje parten tillhandahåller — är det fråga om t.ex. sådana ingripande åtgärder som vid telegrambefordran eller endast direkt överföring som vid fax — skulle kunna leda till slumpartade resultat, där valet av teknisk lösning blir avgörande.

Mera allmänt sett skulle en tillämpning av telegramregeln på elektroniska meddelanden också innebära en återgång i denna del till den s.k. viljeteorin, en återgång som skulle få allt större genomslag i takt med övergången från traditionell till elektronisk kommunikation. En sådan tolkning skulle alltså leda till bedömningar som är oförenliga med huvudreglerna inom avtalsrätten;[54] principen att mottagaren bär risken för befordringsfel står i motsättning till lagens allmänna strävan att i omsättningens intresse skydda godtroende medkontrahent.[55]

Enligt min mening skall sålunda inte någon av reglerna i 32 § AvtL anses tillämpliga på fel som uppkommer när meddelanden överförs

m.m. En direkt medverkan av en fysisk person ersätts därvid av automatiska tredjepartstjänster med en komplexitet och effektivitet som vida överstiger t.ex. överbringande via telegraf. Den tekniska utrustningen kan delvis sägas fungera som en slags "mellanman" som kan "handla" fel.

[52] Se avsnitt 3.3.6.

[53] Härvid agerar knappast någon fysisk person på meddelandenivå, men fel i datorprogram och andra tekniska hjälpmedel kan leda till att texten blir förvanskad. Det kan ofta vara svårt eller omöjligt att avgöra om felet uppkommit till följd av en direkt åtgärd av en person hos det företag som tillhandahåller tjänsten — jfr telegrafisten — eller till följd av fel i de automatiska rutinerna, och oförutsebara variationer kan leda till att meddelanden antingen inte alls kommer fram eller kommer fram i förvanskat skick.

[54] Jfr Håstad, T., Reform av de nordiska avtalslagarna, Forhandlingerne på Det 32. nordiske juristmøde i Reykjavik 1990, Del 1, s. 297.

[55] Grönfors, a.a., s. 200 f.

elektroniskt.[56] Frågan är då om bestämmelsen i 40 § AvtL är ändamålsenligt utformad i ljuset av den ökande användningen av elektronisk kommunikation. Här är en jämförelse med rättsutvecklingen inom köprätten av intresse.

I en motsvarande bestämmelse i 1905 års köplag (61 §) reglerades endast fall där meddelanden försenas eller inte alls kommer fram; jfr 40 § AvtL. Motsvarande bestämmelse i 1990 års köplag (82 §) omfattar emellertid även förvanskning av meddelanden. Frågan om vem som står risken för ett meddelande som avsänts på ett ändamålsenligt sätt har alltså i 82 § köplagen sorterats utifrån typen av meddelande (i stället för sättet för kommunikation) och närmast slumpmässiga variationer, beroende på om hela meddelandet förstörs eller om det endast förvanskas, har kunnat undvikas.

Jag föreslår att 40 § AvtL i detta avseende utformas på samma sätt som 82 § köplagen. En förvanskning som uppkommer under befordran av en handling som har avsänts på ett ändamålsenligt sätt bör bedömas på samma sätt som när meddelandet fördröjs eller inte kommer fram. Genom att 40 § AvtL utformas på detta sätt framgår det motsatsvis att avsändaren bär risken för förvanskning av meddelanden som inte omfattas av den paragrafen.[57]

Mitt förslag innebär att frågan om riskfördelning mellan avsändare och mottagare vid förvanskning av viljeförklaringar och andra meddelanden klargörs. Därvid kan knappast några ökade kostnader uppstå för t.ex. företag och myndigheter — det är en fördel att rättsläget i denna del klarläggs.

I detta sammanhang förtjänar också att uppmärksammas att tiden kan sägas ha runnit ifrån sådana omfattande friskrivningar från ansvar på teleområdet som godtogs vid avtalslagens tillkomst.[58] Denna fråga får dock tas upp i annan ordning.

[56] Annorlunda, naturligtvis, i det fallet att ett elektroniskt meddelande vid avsändandet innehåller ett sådant fel som avses i första stycket.

[57] Eftersom frågan inte behandlas bland ogiltighetsreglerna tillgodoses också behovet av att i s.k. EDI-avtal eller särskilda kommunikationsavtal kunna träffa överenskommelser om fördelningen av risken för förvanskning, genom att det inte längre skulle råda någon tvekan om att avtalsfrihet råder på området (jfr Sisula-Tulokas, L., Datatransmissioner och riskfördelningen för befordringsfel, Festskrift till Kurt Grönfors, s. 408 f. med hänvisningar).

[58] Jfr. 36 § AvtL och Grönfors, a.a., s. 201.

9 Övriga frågor

9.1 Köp och hemförsäljning, m.m.

De köplagsfrågor som aktualiseras i anknytning till IT torde vanligtvis röra ett så sent stadium av parternas mellanhavande att helt automatiska rutiner inte är aktuella. Inte heller i övrigt har jag funnit skäl att i detta sammanhang närmare gå in på regleringen i 1990 års köplag.

Beträffande hemförsäljningslagen (1981:1361) aktualiseras frågan om regler om ångerrätt m.m. är tillämpliga på försäljning med stöd av databaser som kontaktas via nät. Härvid kan ljud, bild och text kombineras till ett synnerligen effektivt medium för försäljning, med direkt kontakt med konsumenter i deras bostad. Kan avtal därvid enligt 1 § första stycket 2 hemförsäljningslagen anses ha ingåtts "vid telefonsamtal som utgör led i försäljning eller annan liknande verksamhet"? Regleringen synes — i vart fall enligt ordalydelsen — inte innefatta sådan försäljning via nät. Inom EU pågår emellertid arbete med ett direktiv som syftar till en tillnärmning av medlemsstaternas lagar och andra bestämmelser om s.k. distansavtal. Med distansavtal avses enligt det nuvarande förslaget till direktiv när en leverantör och en konsument ingår avtal om varor eller tjänster och uteslutande använder en eller flera tekniker för distanskommunikation för att ingå avtalet. Som exempel på sådana tekniker nämns bl.a. e-post och telefax. Vilka följder ett eventuellt direktiv kan komma att få för den svenska lagstiftningen är för tidigt att säga. Om det nuvarande förslaget till direktiv antas, kan man emellertid räkna med att hemförsäljningslagen måste ändras.

Inte heller beträffande skuldebrevslagen finns skäl att här göra någon närmare genomgång. Lagen är allmänt hållen och vissa bestämmelser anses uttrycka i allmänhet tillämpliga rättssatser. Det är härvid möjligt att använda även IT-baserade skuldebrev som är ställda till viss man, dvs. enkla skuldebrev. Löpande skuldebrev baseras däremot på en användning av fysiska originalexemplar och denna funktion kan i vart fall inte för närvarande återskapas i IT-miljön. Databehandlingen baseras, som framgått, på ständiga kopieringar av data som representerar en viss handling.

9.2 EDI inom tillverkningsindustrin

Att de rättsliga förutsättningarna förändras i anknytning till nya IT-baserade handelsmönster framträder särskilt tydligt inom tillverkningsindustrin. Här har datoriseringen gått så långt att handelsparter ofta, i stället för att överföra fullständiga fakturor och andra elektroniska dokument med vedertagna uppgiftskonstellationer, överför uppgifterna successivt mellan informationssystem i takt med godsflöden etc. Det ses som rationellt att inte alls upprätta eller att låta gäldenären upprätta den dokumentation i form av bl.a. fakturor som borgenären vanligtvis ställer ut och översänder till köparen.[59]

De olika rutinerna kan beskrivas utifrån fyra typfall, där utvecklingen går från det första mot det fjärde typfallet.

Det *första typfallet* består i huvudsak av en översättning av traditionella rutiner till IT-miljön så att traditionell dokumentation genereras och översänds, fast i elektronisk form. Än så länge synes utbudet av programvaror för kontroll och uppföljning av kundfordringar och leverantörsskulder vara byggda på sådana rutiner.

I det *andra typfallet* erhåller en handelspart vid skilda tillfällen handlingar som tillsammans upptar den information som t.ex. en traditionell faktura brukar innehålla. De handlingar som tillsammans upptar uppgifterna kan utgöras av t.ex. EDI-avtal, följesedel och prisöverenskommelse. Härvid blir gränsen mellan mottagen och egenupprättad handling oklar och det kan bli svårt att bestämma handlingens bevisvärde, bl.a. eftersom det inte enkelt kan överblickas om en viss uppgift tillförts handlingen av sändaren eller mottagaren. Frågan om utställare av uppgifterna är avgörande för bl.a. äkthetsprövningen.

Det *tredje typfallet* innebär att handelsparter ingår avtal om rutiner för t.ex. leverans och betalning så att åtgärderna knyts till varuflödet. I huvudsak översänder säljare och köpare inga handlingar som bekräftar affärshändelserna utan leverans sker direkt till montering, utan ankomstkontroller. Betalning erläggs direkt i förhållande till tillverkarens produktionsresultat. Det förekommer till och med att leverantören tillåts själv lyfta fordrat belopp från ett köparen tillhörigt konto.

Som ett *fjärde typfall* kan nämnas rutiner som knyter an till ett senareläggande av äganderättsövergången till en vara. Övergången av äganderätten från grossist till yrkesmässig förbrukare av varan eller till detaljist knyts vanligtvis till varans förbrukande eller försäljning i nästa led och administreras genom automatiska rutiner, knutna till t.ex. systemen för materialhantering.

Parterna automatiserar alltså sin kommunikation och fragmenterar den genom stegvisa delmeddelanden, samtidigt som modern teknik kan användas så att parterna, jämfört med traditionella rutiner, har lika mycket eller mer information åtkomlig. Härvid förekommer såväl automatiskt genererade avtalsslut som åtgärder via telenät där handelsparters dokumentation av affärshändelser direkt uppdateras. Till grund för rutinerna ligger vanligtvis EDI-avtal, prisöverenskommelser, etc. Dessa överenskommelser styr uppgiftslämnandet och tidpunkterna härför på ett sätt som avviker från de rutiner som lagts till grund för utformningen av den civilrättsliga regleringen.

[59] Intresset för att effektivisera genom nya organisationsformer och långvarigt nära samarbete mellan olika juridiska personer har ökat. Företagen strävar efter att ändra arbetsfördelningen mellan köpare och säljare och att förkorta leveranstiderna m.m. så att det blir möjligt att arbeta med en mer kundorienterad produktion och att förenkla administrationen så att den till viss del byggs in i processen för varuproduktion.

När borgenären inte utfärdar någon faktura aktualiseras t.ex. frågor om vem det åligger att reklamera och mot vad, samt när en fordran skall anses vara förfallen till betalning, se 4 § räntelagen (1975:635). Till detta kommer frågor om hur en part skall kunna styrka t.ex. ett betalningsanspråk när traditionella bevismedel i form av inkomna fakturor m.m. saknas.

Behovet av rättsliga anpassningar på området bör i huvudsak kunna tillgodoses genom avtal mellan parterna. En framtida användning av sådana rutiner i stor skala torde dock förutsätta en närmare genomlysning av civilrättsliga regelverk, och parterna kan naturligtvis inte genom avtal förfoga över frågor som rör tredje mans rätt. I typfall tre och fyra är det i de flesta fall sannolikt att säljarens rätt till det sålda godset får vika till förmån för köparens borgenärer, och det oavsett om parterna har avtalat att äganderätten inte skall gå över förrän varan har förbrukats eller levererats vidare. Eftersom betalningsfristen kommer att räknas först från sistnämnda händelse föreligger här en risk att leverantörerna, om en köpare går i konkurs, gör ännu större förluster än vid sådana rutiner som berörs i typfall ett och två.[60]

Vidare kan den s.k. varannanlänksprincipen i bokföringslagen och föreskrifterna i mervärdesskattelagen om krav på utfärdande av faktura vålla en del svårigheter vid en övergång till helt elektroniska eller s.k. fakturalösa rutiner. Bokföringslagen ses över av Redovisningskommittén (dir. 1991:71), som beräknas avge sitt slutbetänkande hösten 1996.

9.3 EDI inom offentlig upphandling

Inom Toppledarforum planeras, som framgått av avsnitt 2.3.1, ett snabbt införande av elektronisk handel för kommuner, landsting och stat. Enligt lagen (1992:1528) om offentlig upphandling skall emellertid anbud och ansökningar om deltagande i anbudsgivning som huvudregel avges skriftligt, och om en sådan åtgärd vidtas muntligt eller genom telegram eller telefax måste den bekräftas genom en egenhändigt undertecknad handling.[61]

Bestämmelserna grundas på EG-direktiv och enligt nuvarande reglering kan en övergång till EDI inte ske utan dubblerade rutiner. Det förefaller emellertid som om detta problem håller på att lösas i samband med kommissionens införlivande av världshandelsorganisationen WTO:s upphandlingsregler i EG:s direktiv. En lagändring skulle

[60] Jfr Kommissionslagskommitténs betänkande Kommission och dylikt (SOU 1988:63), s. 95 f.

[61] Se 1 kap. 19 §, 2 kap. 17 §, 3 kap. 22 §, 4 kap. 22 §, 5 kap. 24 § och 6 kap. 3 § lagen om offentlig upphandling.

under gynnsamma omständigheter kunna vara i kraft redan under detta år. Jag föreslår därför inga åtgärder i denna del.

Vid elektronisk kommunikation aktualiseras också frågor om hur regler om öppnande av försändelser bör tillämpas. Försändelser med anbud behöver vanligtvis skyddas från insyn till anbudstidens utgång.[62] Sådana frågor bör dock med nuvarande tekniska möjligheter kunna lösas utan författningsändringar.

[62] Se bl.a. 1 kap. 20 § lagen om offentlig upphandling.

Avdelning III
Elektroniska förmedlingstjänster

10 Utgångspunkter

10.1 Vad är en elektronisk förmedlingstjänst?

10.1.1 Allmänt

Sverige är ett av världens mest datoriserade samhällen. Datorerna har, genom att bindas ihop via telenät och andra kommunikationsleder, blivit länkar i ett globalt system för information, kommunikation, m.m. Sverige befinner sig i frontlinjen också när det gäller de fysiska kommunikationsnätens infrastruktur för överföring av data. Användningen av modern informationsteknik (IT) på data- och teleområdet har bidragit till en ökad internationalisering där traditionella geografiska gränser effektivt bryts igenom. På motsvarande sätt har de nya rutinerna för informationsbehandling delvis suddat ut gränserna mellan olika medier och kommunikationssätt.[1]

Som framhålls i mina direktiv har denna utveckling inneburit ökade möjligheter att enkelt och billigt sprida information med hjälp av datorer. Ett led i denna utveckling har blivit upprättandet av databaser med möjlighet för stora grupper av användare att tillföra databasen egna meddelanden och att läsa andras meddelanden, s.k. elektroniska anslagstavlor eller med en engelsk term Bulletin Board Systems (BBS), som direkt översatt blir ungefär "anslagstavlesystem". Utvecklingen av ny teknik och nya rutiner går dock mycket snabbt, och beteckningen BBS framstår därför delvis som föråldrad. I det följande använder jag därför uttrycket "tjänster för förmedling av elektroniska meddelanden" för att innefatta alla de företeelser som mitt uppdrag avser. Genom sådana förmedlingstjänster skapas helt nya möjligheter att, oberoende av geografiska avstånd, tillgodose intresset av att kunna kommunicera.[2]

[1] Som exempel kan nämnas att radio, TV, kabelkommunikation, telekommunikation och datorkommunikation har uppfattats som klart åtskiljbara företeelser som enkelt kunnat sorteras utifrån såväl informationsinnehåll som användningssätt. Dessa gränser mellan kommunikationsformer, informationstjänster, m.m. har delvis suddats ut genom IT-rutiner där tal, text och bild kan integreras. Traditionella former för kommunikation har fått IT-baserade motsvarigheter. Samtidigt har nya kommunikationsformer och nya mönster för att använda dessa vuxit fram; jfr prop. 1995/96:125 s. 7 f.

[2] Det finns inga säkra siffror rörande omfattningen av den kommunikation som äger rum via elektroniska anslagstavlor men uppskattningar tyder på att det skulle finns mellan 4 000 och 6 000 sådana anslagstavlor i Sverige.

De elektroniska förmedlingstjänsterna har emellertid öppnat vägar också för brottsliga eller i övrigt klandervärda förfaranden.

10.1.2 Teknik, m.m.

När datorer och annan teknisk utrustning kopplas samman så att data kan föras från en punkt till en annan brukar man tala om ett *nät*. Man skiljer därvid mellan lokala nät och fjärrnät.[3] Överföringen av telemeddelanden sker vanligtvis via allmänt tillgängliga telenät. Nät för kommunikation inom företag (s.k. privata nät) och överföring via etern har emellertid fått en allt större betydelse. Datorer, telenät och annan teknisk utrustning erbjuder härvid endast "utrymmen" för att överföra, behandla och lagra data som representerar elektroniska meddelanden.[4]

Förenklat kan den miljö som vuxit fram i anknytning till de elektroniska förmedlingstjänsterna beskrivas utifrån en grundfunktion med en dator försedd med en anslutning till telenätet. Genom att denna dator förses med en viss typ av program för kommunikation kan alla som har tillgång till nätadressen föra in uppgifter och läsa vad andra har lagrat. Det föreligger därmed en elektronisk förmedlingstjänst, vars syfte kan vara att fungera som en "mötesplats" där många kan föra in text eller andra typer av informationsobjekt, samt ta del av varandras texter m.m. Den som driver ett sådant meddelandesystem brukar kallas systemoperatör medan de som anropar (ringer) kallas användare.

För sådana förmedlingstjänster finns en mängd datorprogram, med delvis olika funktioner. Det är här som skillnaderna framträder för användarna. Vanligtvis innehåller sådana programvaror också funktioner för att sända respektive hämta datorfiler. En annan funktion påminner om de texttelefoner som hörsel- och talhandikappade använder. Efter ett elektroniskt anrop till systemoperatören eller en annan användare kan två personer från var sin terminal skriva text direkt till varandra. Genom att tillföra datorprogrammen ytterligare funktioner blir det möjligt att t.ex. adressera ett meddelande till en viss mottagare. Med sådana program för elektronisk post kan en avsändare sända ett meddelande till mottagarens elektroniska adress. Endast mottagaren avses ges tillgång till meddelandet. Efter hand har informationssystemen byggts ut med allt fler funktioner.

[3] När nätet för överföring är konstruerat för analog signalering, krävs särskild utrustning, s.k. *modem*, för översättningen mellan digital och analog representation. Avsändarens modem översätter de digitala signalerna till sådana analoga signaler som kan befordras via telenätet varefter dessa signaler konverteras av mottagarens modem åter till digitala signaler. Telekommunikation digitaliseras emellertid i allt högre grad; jfr Integrated Services Digital Network (ISDN).

[4] För överföringen av data krävs överenskommelser om bl.a. tillämpliga koder, driftsslag, överföringshastighet m.m. Dessa rutiner omvandlas till datorprogram som styr informationsöverföringen.

I syfte att reducera kostnader för telekommunikationer förekommer en överföringsmetod som påminner om kedjebrev. Det finns knutpunkter nära användarna som dessa kommunicerar med. Därifrån sänds informationen vidare till mer centralt belägna datorer, som i sin tur för informationen vidare till en dator för hela landet. Sedan överför denna rikstäckande dator information till datorer i andra länder.[5]

10.1.3 Terminologi och användningssätt

De elektroniska förmedlingstjänsterna kännetecknas av en mångfasetterad användning och en splittrad terminologi. Den kommersiella förmedlingen av information kallas vanligtvis databastjänster eller onlinetjänster, medan ideell verksamhet och liknande initiativ ofta beskrivs med förkortningen *BBS*, som övergripande begrepp under vilket samtliga funktioner sorterar.[6] Bakom de olika begreppen döljer sig delvis olika ändamål och användningssätt för en i grunden likartad men flexibel teknik.

Varje försök att dela in tillämpningarna i t.ex. seriösa kontrollerade elektroniska förmedlingstjänster till skillnad från oseriösa "klotterplank" eller liknande generaliseringar är dömda att misslyckas. Även inom ramen för den kommersiella och forskningsinriktade användningen av förmedlingstjänster förekommer oseriösa eller direkt straffbara inslag, samtidigt som små ideellt drivna BBS:er, vars innehåll inte kontrolleras, kan uppfylla högt ställda etiska krav.

Det finns emellertid olika "kulturer" hos skilda grupper av användare, något som återspeglas också i valet av termer. Skillnaderna är så genomgripande att det kan vara svårt att gemensamt beskriva de elektroniska förmedlingstjänsterna. I det följande görs dock ett försök att strukturera de former för datorförmedlad kommunikation som är av betydelse för mitt uppdrag.

Elektronisk post (e-post, Electronic Mail, e-mail) innebär i sin grundform att den som sänder ett meddelande anger namn och elektronisk adress till en eller flera mottagare, och att det elektroniska brevet sedan överförs till mottagarnas elektroniska brevlådor; jfr att sända ett traditionellt brev till en viss adressat. En brevlåda kan sägas vara den komponent i meddelandesystem som kommunicerar med andra brevlådor för att överföra meddelanden; jfr min användning av uttrycket elektronisk adress i avdelning I. Meddelandehantering brukar beskrivas som en kombination av meddelandeöverföring och meddelandelagring.

[5] Detta förfarande har i bland kallats "echo-mail", meddelanden "ekas" från en dator till en annan. Som exempel på ett sådant nät kan nämnas Fidonet.

[6] Begrepp som elektronisk anslagstavla, elektroniskt klotterplank och elektronisk post förekommer också i dessa sammanhang.

Distributionslistor (Mailing Lists) är en tilläggsfunktion till e-post, som innebär att en avsändare, i stället för att sända meddelandet till uppräknade mottagare, sänder det till listans elektroniska adress. Denna adress leder till en automatiskt fungerande enhet som styrs av en lista över medlemmarnas elektroniska adresser och sänder inkomna meddelanden vidare till dessa. Distributionslistan utgör således ett medel för gruppkommunikation genom att meddelanden sänds vidare som elektronisk post till dem som upptas i listan.

Ett datorstött *konferenssystem* utgörs av en databas av meddelanden, uppdelad på olika "möten" över olika ämnen där kommunikationen inte sker i realtid (dvs. inte sker samtidigt). Användarna kan lägga in meddelanden i möten och läsa vad andra har skrivit. Mötet kan därmed bli ett medium för diskussion mellan deltagarna. Konferenssystem är alltså även de ett medel för gruppkommunikation. Observera att alla gruppdeltagarna inte behöver vara med samtidigt, som vid vanliga möten. Deras meddelanden lagras i datorn, och kan läsas senare. Var och en kan delta vid en tidpunkt som passar honom. En distributionslista eller ett konferenssystem fungerar oftast som ett diskussionsforum och ett medel för erfarenhetsutbyte mellan medlemmarna. Mindre, slutna grupper kan fullgöra funktioner jämförliga med sammanträden, arbetsgrupper och studiecirklar.

Vissa system tillhandahåller en s.k. *nyhetskontroll*, varmed avses en mekanism som hjälper den som söker information att hitta det som är nytt och som han ännu inte har läst. En sådan mekanism är vanlig i fråga om elektronisk post, distributionslistor och konferenssystem, men är mindre vanlig i databaser baserade på fritextsökningar eller sådana hänvisningar som beskrivs nedan.

Distributionslistorna och konferenssystemen har ibland en s.k. *moderator*, ett slags ordförande med behörighet att ta bort irrelevanta inlägg ur mötet. Det förekommer också att moderatorn, beträffande grupper med ett stort antal medlemmar, måste läsa och godkänna meddelanden innan de görs tillgängliga för medlemmarna. Det vanligaste är dock att mötena inte har någon moderator. Grupperna kan vara *slutna* (dvs. alla släpps inte in) eller *öppna* (alla som vill får vara med). Varianter, där grupper är öppna för vissa användargrupper (t.ex. anställda i ett företag) och slutna för andra, förekommer också.

Med *elektroniskt meddelande* förstås allt oftare inte bara text, utan också bilder och annan information. Ljud och rörliga bilder (animation och video) förekommer och kan väntas bli vanliga i framtiden. Meddelanden lagras ofta så att de kan *sökas* av en person som letar efter information. Vanliga sätt att organisera sådana förmedlingstjänster är genom *hänvisningar* till meddelanden. Läsaren kan genom att följa hänvisningarna "bläddra" eller "surfa" på nätet från meddelande till meddelande. Två vanliga varianter av sådana hänvisningar är *menyer* (listor över dokument, där användaren kan välja något av dem) och s.k.

hyperlänkar (texten i ett dokument innehåller "klickbara fält" som leder vidare till andra dokument; jfr nedan angående World-Wide Web). Såväl menyer som hyperlänkar kan leda vidare till nya dokument som i sin tur innehåller menyer och hyperlänkar och användaren kan därigenom sekundsnabbt förflytta sig mellan olika förmedlingstjänster, som kan finnas i olika världsdelar. En annan vanlig form är att meddelanden kan *sökas på ord* eller kombinationer av ord i deras filnamn, rubriker eller i hela texten.

Datorprogram utgör en viktig kategori av objekt som användare kan skicka till varandra via elektroniska förmedlingstjänster. De flesta sådana program får fritt kopieras via nät (s.k. Shareware, någon svensk term finns inte), men det kan också förekomma att upphovsrättsligt skyddat material såsom piratkopior av datorprogram och artiklar ur tidningar sprids utan upphovsmannens tillstånd. För att förenkla framställningen innefattar jag i det följande också datorprogram under uttrycket elektroniskt meddelande.

Olika slag av begränsningar beträffande åtkomsten till elektroniska förmedlingstjänster (*accesskontroll*) kan förekomma. Vissa system delar strikt upp sina användare i informationslämnare (som kan ändra i databaserna) och informationsmottagare (som kan läsa, men inte ändra). Det vanligaste är emellertid att alla användare har möjlighet att både skriva och läsa.

De elektroniska förmedlingstjänsterna kan vara mer eller mindre *styrda uppifrån* (av den som tillhandahåller tjänsten) eller *styrda underifrån* (av användarna). Kommersiella system är ofta mera uppifrånstyrda, medan system som drivs på ideell basis, inklusive Internet och Fidonet, är utpräglat underifrånstyrda: Användare har vanligtvis möjlighet att starta egna grupper, gå med i öppna grupper, skriva inlägg i grupperna, lägga upp information för åtkomst i databaser etc.

Det blir allt vanligare att förmedlingstjänsterna är distribuerade, alltså spridda på många olika datorer i ett nät. Distributionen kan ske genom replikering, alltså att meddelanden kopieras ("ekas") från *värddator* (server) till värddator, så att användarna kan hitta sin information i en lokal värddator, även när informationen ursprungligen kommer från någon annan dator i nätet. I andra fall sker distributionen genom att användaren hämtar meddelanden från deras ursprungliga förvaringsplats, men att hänvisningar finns som hjälper användaren att "bläddra" och "söka" information även om den är spridd på många datorer och förmedlingstjänster.

En värddator som användare kan koppla upp sig till tillhandahåller vanligtvis flera olika funktioner av det slag som behandlats ovan. En sådan elektronisk anslagstavla kan beskrivas som en värd till vilken flera användare elektroniskt kan koppla sig via nät. En elektronisk anslagstavla kan tillhandahålla många olika tjänster till sina användare,

t.ex. elektronisk post, konferenssystem med öppna och slutna möten och databaser med hyperlänkar eller ordsökning. Ofta tillåter den elektroniska anslagstavlan att användarna både lämnar och hämtar information. Informationen kan bestå av t.ex. diskussioner, utredningar, noveller, dikter, artiklar, bilder och programvaror — i princip all slags information kan distribueras via elektroniska anslagstavlor. Många elektroniska anslagstavlor är kopplade i nät.

World-Wide Web (www) är en funktion inom ramen för Internet där användarna på ett enhetligt sätt kan ta del av och hämta information i form av ljud, text och bild från olika förmedlingstjänster. Användaren kan med hjälp av hyperlänkar enkelt förflytta sig mellan olika tjänster, oberoende av i vilka länder de datorer finns via vilka tjänsterna tillhandahålls.

En kontroversiell företeelse är s.k. *anonymitetsservrar*. En sådan fungerar vanligen så att den tar emot meddelanden, byter ut avsändarens namn och adress mot en pseudonym och sänder meddelandena vidare. De flesta servrar lagrar en tabell som kan översätta mellan riktiga adresser för e-post och pseudonymer. Denna tabell används för att det skall bli möjligt att ta emot brev till en pseudonym och förmedla det vidare till den verklige avsändarens elektroniska adress. Givetvis kan en sådan tabell, om den blir tillgänglig för polisen, också användas för att spåra brottsliga meddelanden.

Som skäl för sådana anonymitetsservrar har anförts att de ger människor möjlighet att diskutera känsliga saker, t.ex. personliga problem, utan att tala om sitt namn. Det har också sagts att dessa servrar gör att personer verksamma vid företag och myndigheter vågar berätta saker som de annars inte yppar, t.ex. information om missförhållanden. Mot sådana servrar har anförts att de underlättar spridning av brottslig information.

Det förutspås en snabb utveckling av elektroniska förmedlingstjänster. Nya nät och nya tjänster växer fram i snabb takt, delvis utan övergripande planering och styrning.[7] Dessa tjänster används visserligen i huvudsak på ett seriöst, eller i vart fall oförargligt sätt. Nya risker framträder emellertid för brottslig eller annars oacceptabel spridning av information genom att data i princip flyter fritt mellan olika meddelandesystem och olika länder. Dessutom ger nya funktioner i datorprogram, som tidigare använts endast för att ta del av elektroniska förmedlingstjänster, möjlighet att enkelt sätta upp egna sådana tjänster.

[7] Som exempel kan nämnas att ingen planerat det globala meddelandesystemet Internet i dess nuvarande form. Systemet, som uppstod ur ett internt kommunikationssätt mellan den amerikanska militärindustrin och universiteten, organiserades av säkerhetsskäl så att det inte skulle finnas något centrum eller någon mittpunkt som kunde slås ut. I dag vet ingen hur stort Internet är, hur många användarna är och hur snabbt systemet växer. Detsamma gäller omfattningen av sådana sammanslutningar som Fidonet där meddelanden kopieras - "ekas" - från BBS till BBS.

Det finns inte underlag för några säkra bedömningar av hur omfattande de kriminella aktiviteterna är. Enligt vad som har upplysts vid utredningens kontakter med Rikspolisstyrelsen torde emellertid sådana aktiviteter förekomma regelbundet inom många elektroniska förmedlingstjänster.

10.2 Vilka rättsfrågor framträder

När elektroniska förmedlingstjänster ställs till förfogande för grupper av användare aktualiseras nya rättsfrågor som ofta bryter igenom traditionella gränser mellan rättsområden och ställer konflikter mellan motstående intressen på sin spets. Framställningen begränsas här till de områden som framstår som särskilt angelägna vid en anpassning av författningsregleringen till elektroniska förmedlingstjänster.[8]

10.2.1 Straffrättsliga frågor

Bakgrund

Elektroniska förmedlingstjänster kan användas i anknytning till en mängd olika brottsliga eller annars oacceptabla förfaranden, och enligt uppgifter från Rikspolisstyrelsen framträder sådana förmedlingstjänster som en ingrediens i huvuddelen av de brottsutredningar som förekommer på IT-området. Särskilt frekventa är förfaranden som syftar till att sprida rasistiska eller annars otillåtna uttalanden eller bilder, att uppmana till och att upplysa om hur brott kan utföras, att bjuda ut stöldgods, narkotika m.m., och att olovligen sprida immaterialrättsligt skyddat material.

Spridning av rasistiska eller annars otillåtna uttalanden, m.m.

Rasistiska och annars otillåtna uttalanden som sprids via elektroniska förmedlingstjänster är vanligtvis förenade med uppmaningar att vidta straffbara åtgärder, bl.a. mot etniska minoriteter. Bestämmelsen i 16 kap. 5 § brottsbalken (BrB) om *uppvigling* kan bli tillämplig om förfarandet innebär att någon i meddelande till allmänheten uppmanar eller eljest söker förleda till brottslig gärning, svikande av medborgerlig skyldighet eller ohörsamhet mot myndighet. Den exemplifierande uppräkningen av sätten för att uppmana till brott m.m. rymmer olika

[8] Diskrimineringsombudsmannen har i en skrivelse till regeringen tagit upp frågor om spridande av främlingsfientliga budskap i elektroniska anslagstavlor. Vidare har Umeå universitet, i en skrivelse till regeringen, mot bakgrund av att pornografiska bilder har spritts via universitetets datanät, anhållit om en genomgång av bl.a. vilka rättsliga åtgärder som kan vidtas när missbruk av detta slag har förekommit. Regeringen har överlämnat den senare skrivelsen till utredningen.

former för kommunikation. Uppvigling avser uppmaningar till en obestämd krets och personkretsen får inte vara på en gång liten och sluten.

När någon i meddelanden som sprids via elektroniska förmedlingstjänster hotar eller uttrycker missaktning för folkgrupp eller annan sådan grupp av personer, med anspelning på bl.a. ras eller etniskt ursprung eller trosbekännelse, aktualiseras bestämmelsen i 16 kap. 8 § BrB om *hets mot folkgrupp*. För att straffbestämmelsens krav på *spridning* skall vara uppfyllt måste det vara fråga om yttranden utanför den helt privata sfären. Är detta uppfyllt torde det räcka att meddelandet når en grupp människor som utgör mer än ett fåtal. Spridandet kan ske genom t.ex. upprepade privata samtal — jfr den spridning som blir följden av att olika personer kopplar upp sig mot en databas med främlingsfientliga meddelanden.

Den som skildrar barn i pornografisk bild med uppsåt att bilden sprids eller som sprider en sådan skildring kan enligt 16 kap. 10 a § BrB dömas för *barnpornografibrott*. Enligt lagmotiven gäller paragrafen alla slag av bilder, även tecknade bilder med barnpornografiskt motiv. I detta sammanhang aktualiseras också 16 kap. 10 b § BrB om *olaga våldsskildring*, en bestämmelse som rör bl.a. bilder där sexuellt våld eller tvång skildras; jfr 16 kap. 11 och 12 §§.

Att uppmana till och att upplysa om hur brott utförs

Det finns elektroniska förmedlingstjänster som innehåller t.ex. recept på narkotika, datavirus och programvaror för att tillverka datavirus, beskrivningar av hur bomber tillverkas, hemliga koder för tillträde till informationssystem, programvaror för att forcera behörighetskontrollsystem samt kontonummer m.m., som kan användas för att begå bl.a. bedrägerier.[9] Detta innebär såväl ett hot mot informationssäkerheten som en inkörsport för ungdomar till brottsliga aktiviteter.

I 23 kap. BrB ges föreskrifter som utvidgar det straffbara området utanför de gränser som dras av brottsbeskrivningarna i de särskilda straffbuden. För de här aktuella situationerna, där utförandet av ett brott inte har påbörjats, återstår att överväga om ansvar för *förberedelse* eller för *stämpling* till brott kan komma i fråga. Datorer och andra hårdvaror aktualiseras som hjälpmedel för brottslig verksamhet, först efter att ha försetts med vissa program eller andra data som är ägnade för brottslig verksamhet. Intresset knyts således till själva data.

[9] Det har också förekommit att företagshemligheter och uppgifter av betydelse för nationell säkerhet har spridits via elektroniska förmedlingstjänster, av hackers som velat bevisa sin förmåga att ta sig in i databaser där sådant material finns; jfr 5 kap. 2 § sekretesslagen (1980:100).

Enligt 23 kap. 2 § BrB består straffbar *förberedelse* till brott — såvitt här är av intresse — i att anskaffa, förfärdiga, lämna, motta, förvara, fortskaffa eller ta annan dylik befattning med gift, sprängämne, vapen, dyrk, förfalskningsverktyg eller annat sådant hjälpmedel. Av denna exemplifierande uppräkning framgår att lagregeln avser traditionella fysiska objekt, inte program och andra data. Ansvar för förberedelse till brott aktualiseras vidare endast i de fall som särskilt anges i respektive kapitel i brottsbalken.

Med stämpling till brott avses bl.a. att någon *söker anstifta* annan att utföra en brottslig gärning. Det finns elektroniska förmedlingstjänster med meddelanden som innefattar direkta uppmaningar att t.ex. "spränga" eller annars vidta integritetskränkande åtgärder mot vissa personer. Uppmaningarna kan ingå i meddelanden mellan två användare av en elektronisk förmedlingstjänst men som alla som hör till den aktuella konferensen kan läsa; jfr ett direkt samtal där många hör vad som sägs.[10] Det har förekommit att tonåringar felaktigt trott sig kommunicera med en jämnårig när äldre personer, som tillägnat sig den jargong ungdomar använder vid kommunikation via elektroniska förmedlingstjänster, använt mediet för att utöva extrem politisk påverkan.

Från straffrättslig utgångspunkt framträder den komplikationen att gärningsbeskrivningarna vanligtvis avser att någon sätter sig i förbindelse med *viss eller vissa personer* för att försöka förmå dem att begå brott. Sådant material i elektroniska förmedlingstjänster som innefattar uppmaningar till brott synes emellertid i många fall vara riktat till en vidare krets, eller riktat till en viss person med den uppenbara avsikten att det skall läsas av alla.

Ansvar för stämpling till brott kan komma i fråga endast i de fall som särskilt anges i respektive kapitel i brottsbalken.

Narkotikabrott, häleri, m.m.

Enligt 1 § 5 narkotikastrafflagen (1968:64) kan den som olovligen bjuder ut narkotika till försäljning, förmedlar kontakter mellan säljare och köpare eller företar någon annan sådan åtgärd, dömas för narkotikabrott, om förfarandet är ägnat att främja narkotikahandel och gärningen sker uppsåtligen. Förberedelse och anstiftan till narkotikabrott är också kriminaliserad (4 § narkotikastrafflagen).

När någon i stället bjuder ut stöldgods eller liknande via en elektronisk förmedlingstjänst uppkommer frågan om någon av bestämmelserna i 9 kap. 6 och 7 §§ BrB om *häleri* och häleriförseelse kan tillämpas.

[10] Sådana uppmaningar kan också förekomma vid den ovan beskrivna tillämpningen där två användare som är uppkopplade samtidigt skriver text till varandra i realtid.

I sammanhanget bör också nämnas bestämmelsen i 4 § lagen (1990:409) om skydd för *företagshemligheter*, enligt vilken den som anskaffar en företagshemlighet med vetskap om att den som tillhandahåller hemligheten eller någon före honom har berett sig tillgång till denna genom företagsspioneri, skall dömas för olovlig befattning med företagshemlighet.

Upphovsrättsligt skyddat material

Det upphovsrättsliga skyddet enligt lagen (1960:729) om upphovsrätt till litterära och konstnärliga verk aktualiseras också i anknytning till elektroniska förmedlingstjänster.

I praktiken är det främst s.k. piratkopiering av datorprogram som har föranlett rättsliga åtgärder. Användningen av datorer har dock fört med sig att företeelser som tidigare enkelt kunnat sorteras utifrån såväl informationsinnehåll som metoder för användning och informationsöverföring flutit samman. Det är tillräckligt att nämna medier där tal, text och bild integreras, samtidigt som det är möjligt att sekundsnabbt förmedla/kopiera data som representerar ett verk.

Genom att ett skyddat datorprogram görs tillgängligt via en elektronisk förmedlingstjänst, kan det spridas i en omfattning och med en snabbhet som är svår att åstadkomma i traditionell miljö. Samtidigt har svårigheter framträtt att lagföra sådan spridning.

Från praxis kan nämnas ett av Högsta domstolen (HD) nyligen avgjort brottmål[11], där HD konstaterade att såväl en olovlig överföring *till* en elektronisk anslagstavla (upload) av ett skyddat datorprogram, som en vidareöverföring av ett sådant program (download) *från* en elektronisk anslagstavla till en annan dator, innefattar intrång i upphovsrätt. Målet gällde emellertid — som talan slutligen utformades — endast frågan om den som drev den elektroniska anslagstavlan gjort sig skyldig till intrång i upphovsrätt redan genom att programmen varit tillgängliga i hans anslagstavla så att de kunnat kopieras genom download av en krets personer som kan anses utgöra allmänheten. Något annat aktivt handlande än det som kunde anses ligga i att den tilltalade tillhandahållit anslagstavlan i syfte att den skulle fungera som dels en elektronisk brevlåda för meddelanden, dels ett lager för program som får distribueras fritt, åberopades inte.

Åtalet lämnades utan bifall på den grunden att ansvar för sådant tillgängliggörande som avses i 2 § upphovsrättslagen förutsätter någon form av aktivt handlande, och att enbart ett tillhandahållande av en elektronisk anslagstavla inte kan anses uppfylla detta krav på aktivt handlande. HD tillade att det därmed föreligger en påtaglig lucka i det upphovsrättsliga skyddet och berörde de elektroniska förmedlings-

[11] HD:s dom den 22 februari 1996, DB 28.

tjänsternas omfattning och svårigheterna att spåra användare som kan göras ansvariga för olovlig kopiering. Dessa problem fick det att framstå som naturligt att i stället enligt gällande rätt söka utkräva ansvar av systemoperatören. HD anförde härvid följande:

Det skulle sålunda kunna tänkas att en systemoperatör görs ansvarig så som medverkande till en användares olovliga kopiering. Med Riksåklagarens nyss angivna förklaring har frågan om ansvar för medverkan saknat aktualitet i målet. Det har inte heller funnits anledning att pröva huruvida en systemoperatör på grund av särskilda förpliktelser eller av annan orsak har en sådan ställning att han kan fällas till ansvar för en underlåtenhet att vidta viss åtgärd, t.ex. att radera ett datorprogram som överförts till hans BBS.

Med den slutsats som dragits i det föregående angående krav på aktiv åtgärd för att systemoperatören skall kunna göras ansvarig för upphovsrättsintrång kan det te sig närliggande att undersöka, om inte en operatör vidtagit någon sådan åtgärd som skulle tillgodose aktivitetskravet. De åtgärder som då skulle kunna komma i fråga är exempelvis sådana som den tilltalade efter hand företagit i syfte att begränsa tillgängligheten till datorprogrammen. För den händelse åtgärder av detta slag, som likväl inte förhindrat en spridning till allmänheten, skulle medföra ett straffansvar, skulle det innebära att den som gör något, om än för litet, skulle anses vara mer klandervärd än den som i ett motsvarande fall bara "sitter med armarna i kors". Från rättspolitisk synpunkt skulle en sådan ordning knappast anses som godtagbar.

Jag återkommer till dessa frågor i avsnitt 12.2.5.

Går det att identifiera en gärningsman?

De berörda straffbestämmelserna har i huvudsak tillkommit vid en tid när kommunikation med användning av datorer inte var aktuell. Lagstiftaren har således utgått från traditionella förutsättningar för att spana, att peka ut en ansvarig och att i övrigt leda brottsliga förfaranden i bevis. IT-användningen har emellertid, i förening med den kultur som vuxit fram bland användarna av elektroniska förmedlingstjänster, gjort det svårt att fastställa från vem ett uttalande, en bild eller ett datorprogram härrör.

Från straffrättslig utgångspunkt är huvudfrågan således vem som bör anses vara ansvarig enligt de aktuella straffbestämmelserna. Frågan har samband med vilka tekniska och administrativa åtgärder som vidtas för att den som använder en elektronisk förmedlingstjänst skall kunna identifieras. Exempel på sådana åtgärder för identifiering är krav på avancerad lösenordshantering, digitala signaturer[12], och kommunikation via pappersbaserade undertecknade handlingar innan en ny användare bereds tillträde till informationssystemet.

Om säkra identifieringsmetoder föreligger torde frågan om vem som bär ett straffrättsligt ansvar knappast vålla svårigheter. En fortsatt utveckling mot kommunikation där kraven på informationssäkerhet m.m. ställs lågt aktualiserar emellertid frågor om ett vidgat straffansvar, eller

[12] En digital signatur ger — vid lämpligt utformade rutiner — möjlighet att verifiera både vem som ansvarar för ett meddelande och om meddelandet har förvanskats, medan lösenord vanligtvis skyddar endast mot att obehöriga bereds tillträde till ett system; se vidare bilaga 2.

om att peka ut någon som straffrättsligt ansvarig för den information som sprids via en elektronisk förmedlingstjänst; jfr den ansvarige utgivaren för en dagstidning. Därvid berörs också frågor om straffprocessuella tvångsmedel m.m.

10.2.2 Straffprocessuella frågor

Svårigheterna att finna en gärningsman beror på att data utan särskilda kontroller tillförs elektroniska förmedlingstjänster via nät. Det har visat sig att den som misstänks för brott med anknytning till en elektronisk förmedlingstjänst som han innehar vanligtvis gör gällande att han inte känner till att aktuella meddelanden finns i basen eller vem som har sänt in dem.

Från en *strikt teknisk utgångspunkt* torde brottslig informationsspridning via elektroniska förmedlingstjänster — till skillnad från t.ex. muntlig kommunikation, flygblad eller telefonsamtal — lämna vissa spår som, om de utnyttjas effektivt, kan leda till gärningsmannen. Det som skrivs i elektroniska diskussionsgrupper och adresser för förmedlingen lagras ju i datorer. Till och med information som raderats i en dator finns ofta kvar.[13] Även om oriktiga uppgifter om avsändare har använts finns det relativt goda *tekniska* möjligheter att spåra källan genom att följa kedjan bakåt i näten.[14]

Det finns emellertid vanligtvis *inte rättsliga förutsättningar* för sådana åtgärder. Spaning som avser elektroniska förmedlingstjänster tangerar tvångsmedel som husrannsakan, beslag, hemlig teleavlyssning och hemlig teleövervakning samt aktualiserar okonventionella metoder och förfaranden; jfr bestämmelsen i 2 kap. 6 § regeringsformen. I den mån en åtgärd blir att bedöma som teleavlyssning eller teleövervakning är användningsområdet, med hänsyn till skyddet för den enskildes personlig integritet, begränsat till sådan grov brottslighet som vanligtvis inte misstänks i de nu aktuella fallen. När husrannsakan och beslag aktualiseras kan i stället proportionalitetsprincipen lägga hinder i vägen för åtgärder som kan framstå som ett kringgående av bestämmelserna om hemlig teleavlyssning och hemlig teleövervakning. Visserligen kan dessa hinder mötas genom tekniska och administrativa åtgärder som underlättar för polisen att få uppgifter om vem som sprider viss information, men tillförlitliga sådana åtgärder är inte vanliga på

[13] Ett välkänt exempel är när Oliver North dömdes för att olagligt ha förmedlat ekonomiskt stöd till Contras i Nicaragua. Som bevis mot honom användes meddelanden som han skrivit i Vita Husets system för e-post och som han trodde var raderade, men som kunde tas fram av åklagaren från band med säkerhetskopior.

[14] För att dessa tekniska möjligheter skall kunna utnyttjas i praktiken krävs det ofta att den som tillhandahåller tjänsten lämnar upplysningar och i övrigt biträder i arbetet.

området för elektroniska förmedlingstjänster, och någon fullständig säkerhet kan inte uppnås.[15]

En annan begränsning följer av telekommunikationernas *internationella karaktär*. Den som för in brottsligt material kan ha kopplat upp sig i många led via flera länder. Det torde utgöra ett intrång i det främmande landets suveränitet om svensk polis självständigt vidtar åtgärder som avser datorer och nät i andra länder.

Användningen av elektroniska förmedlingstjänster aktualiserar således grundläggande och principiella frågor som har samband med brister i IT-anpassningen av den straffprocessuella regleringen. Dessa frågor, som delvis torde kunna lösas endast genom internationella överenskommelser, bör behandlas i ett större sammanhang.[16] Här tas endast upp de speciella frågor som användningen av elektroniska förmedlingstjänster aktualiserar.

Eftersom metoderna för kommunikation m.m. via elektroniska förmedlingstjänster är okonventionella, kan frågor om *okonventionella spanings- och utredningsmetoder* beröras. Utrymmet för sådana metoder är dock begränsat och de principer som anses gälla på området är inte lättillgängliga. Förfaranden, som för tanken till s.k. infiltration eller till förtäckt husrannsakan, torde över huvud taget inte få förekomma inom ramen för den öppna polisverksamheten.

Ett exempel från England visar emellertid hur svårigheterna att påvisa brott med anknytning till elektroniska förmedlingstjänster föranlett ovanliga åtgärder. En stiftelse har bildats för att tillvarata programvaruföretagens intressen. Den arbetar praktiskt t.ex. så att någon för stiftelsens räkning men i eget namn anmäler sig som användare vid en elektronisk förmedlingstjänst där olovlig spridning av upphovsrättsligt skyddat material antas förekomma. Användaren hämtar och sparar det material som behövs från förmedlingstjänsten för att styrka brott. Därvid förekommer också att användaren kommunicerar med systemoperatören och — genom elektroniskt förmedlade frågor och svar som loggas[17] — inhämtar besked varav avses framgå om system-

[15] De uppgifter som behövs för ett åtal kan i bästa fall återfinnas vid en utvärdering av material som har beslagtagits. För dessa åtgärder krävs såväl tekniska kunskaper som kännedom om hur systemen brukar användas. Numera finns dock viss expertis inom de brottsutredande organen när det gäller vad som bör tas fram och "var" uppgifter av intresse kan finnas.

[16] Frågorna har behandlats av Datastraffrättsutredningen vars synsätt rörande husrannsakan och beslag i princip har genomförts med avseende på tvångsmedlen inom ramen för skatterevisioner (prop. 1993/94:151 s. 256). Vissa förslag till anpassning av bestämmelserna om hemlig teleavlyssning och hemlig teleövervakning har också genomförts, (prop. 1994/95:227). Vidare har Polisrättsutredningen, med avseende på traditionell miljö, i betänkandet Tvångsmedel enligt 27 och 28 kap. RB samt polislagen (SOU 1995:47) lämnat vissa allmänna synpunkter på hur en processuell reglering för IT-miljön bör utformas, men utan att i den delen presentera några författningsförslag.

[17] Med en terminologi övertagen från sjöfartens loggböcker används begreppet *logg* som beteckning på en regelbundet gjord uppteckning av händelser som inträffar under drift av databehandlingssystem.

operatören är införstådd med eller ovetande om de brottsliga aktiviteterna. När stiftelsen överlämnar materialet till polisen är utredningen i stora delar redan gjord; jfr de svenska försäkringsbolagen som har personal avdelad för att vidta åtgärder med anledning av misstankar om försäkringsbedrägeri.

Utanför området för immaterialrättsligt skydd saknas dock vanligtvis resursstarka intressenter, och polisanmälningar eller annat underlag för åtgärder torde höra till undantagen. Detta gäller bl.a. brottslig spridning av barnpornografi och främlingsfientligt material samt annonsering för försäljning av narkotika och vapen.

Åtgärder av polisen kan också aktualisera *straffrättsliga frågor*. Det är oklart i vilken omfattning bestämmelserna om straff för intrång i information medför krav på beslut om användning av tvångsmedel. Det förekommer bl.a. att bilden, vid uppkoppling till elektroniska förmedlingstjänster där ingen manuell kontroll sker, innehåller beskedet att poliser inte äger tillträde. Skall den polis som kopplar upp sig därvid anses ha gjort sig skyldig till ett brottsligt förfarande?

10.2.3 Skyddet mot otillbörligt integritetsintrång

I datalagen (1973:289) ges skydd mot otillbörligt intrång i den enskildes personliga integritet till följd av att personuppgifter registreras med hjälp av ADB. Denna reglering har redan behandlats i avsnitt 6.3 med avseende på myndigheternas elektroniska dokumenthantering. I det följande tar jag upp de ytterligare frågor som uppkommer i anknytning till elektroniska förmedlingstjänster.

När en stor mängd användare fritt kan påverka registrens innehåll och använder dem för olika syften aktualiseras bl.a. frågor om registeransvar och ändamålsbestämning. Skall hela förmedlingstjänsten ses som ett enda register i datalagens mening? Särskilt tydligt framträder denna fråga i 7 a § DL (jfr 15 kap. 11 § sekretesslagen) där det föreskrivs att det hos den registeransvarige skall finnas en förteckning över de personregister som han är ansvarig för. Det är uppenbart att en sådan regel är svår att förena med att andra än den som är ansvarig för förmedlingstjänsten tillåts starta nya konferenser där ändamålet för dataregistreringen är ett annat än för tjänsten i övrigt. Vidare har bestämmelsen om registeransvar utformats så att varje användare av en förmedlingstjänst, vid en strikt tolkning, skulle kunna bli ansvarig (1 § DL).

Personregister som inrättas och förs uteslutande för personligt bruk undantas från såväl licens- som tillståndsplikten enligt datalagen. I mina direktiv sägs att enskilda som uteslutande för personligt bruk inrättar och för elektroniska anslagstavlor inte torde omfattas av datalagens

regler om licens- och tillståndsplikt[18] men att en näringsidkare eller en myndighet som vill inrätta en sådan elektronisk anslagstavla med möjlighet att bearbeta personuppgifter ställs inför frågan om detta också innebär att ett personregister i datalagens mening inrättas. Enligt utredningsdirektiven torde många elektroniska förmedlingstjänster sannolikt behöva prövas enligt DL:s regler.

I datalagen föreskrivs vidare att insamling, registrering, utlämnande och användning av uppgifter skall ske i överensstämmelse med registrets ändamål. Regleringen baseras därvid på att den registeransvarige har full kontroll över databehandlingen, en situation som självklart förelåg vid datalagens tillkomst. På området för elektroniska förmedlingstjänster synes ett sålunda utformat registeransvar förutsätta någon form av förhandsgranskning av de uppgifter som tillförs en elektronisk förmedlingstjänst. Som framgått är en förhandsgranskning dock svår att genomföra och förena med syftet bakom den form av öppet forum för åsiktsutbyte som en elektronisk förmedlingstjänst vanligtvis utgör.[19] Även bestämmelserna om rättelse m.m. och om att på begäran underrätta den som är registrerad om innehållet i de personuppgifter om honom som ingår i registret bygger på att den registeransvarige har full kontroll över informationsbehandlingen. Det är inte enkelt att komma tillrätta med spridning av felaktiga uppgifter när uppgiftslämnare, minuten efter att en felaktighet har korrigerats, elektroniskt kan föra in nya meddelanden med samma innehåll. På motsvarande sätt kan underrättelseskyldigheten i 10 § DL bli overksam eftersom den registeransvarige knappast kan styra informationsbehandlingen så att personuppgifter som rör en viss person generellt kan tas fram.[20] Åtgärder för att vidga möjligheterna till sådana sökningar skulle dessutom föra med sig en utformning av rutinerna som är betydligt känsligare från integritetssynpunkt, eftersom sådana rutiner också kan användas för databehandling som innebär nya risker för otillbörligt integritetsintrång.

Andra bestämmelser som skapar tillämpningssvårigheter är föreskrifterna om förbud mot utlämnande om det finns anledning att anta att uppgiften skall användas för ADB i strid mot datalagen eller mot

[18] Jfr Sundsvalls tingsrätts dom den 2 november 1993, DB 728.

[19] Man kan något tillspetsat ställa frågan hur någon skall kunna se till att registerändamålet följs när det ligger i ändamålet med en elektronisk förmedlingstjänst att en sådan kontroll inte äger rum; jfr de förmedlingstjänster där användarna själva får starta nya konferenser och begränsa åtkomsten till en viss krets av deltagare. Bestämningar av registerändamålen för elektroniska förmedlingstjänster synes därvid delvis ha omöjliggjorts. Man kan visserligen tänka sig att den som inrättar en ny konferens från början beskriver ändamålet och att varje konferens ses som ett register i sig, i vart fall när konferensen är sluten, men det är inte ovanligt med inlägg som faller utanför avsedd ram och varje användare som tillhör en konferens brukar fritt kunna föra in nya inlägg.

[20] Det är mycket vanligt med täcknamn eller pseudonymer (s.k. "handles") och ofullständiga men för den aktuella kretsen helt begripliga förkortningar eller påhittade beteckningar för en viss person.

utlämnande, utan medgivande av Datainspektionen, om uppgiften kan antas bli använd för automatisk databehandling i utlandet och det inte rör sig om ett land som har anslutit sig till Europarådets dataskyddskonvention, 11 § DL; jfr 7 kap. 16 § sekretesslagen (1980:100). Inte ens alla EU-stater är anslutna till dataskyddskonventionen. Om bestämmelsen skall iakttas kan inte var och en tillåtas att utan kontroller hämta uppgifter från systemet. Personuppgifter kan inte heller fritt sändas från ett personregister i Sverige via t.ex. CompuServe eftersom de då lämnas ut till USA och databehandlas där så att de förmedlas till adressaten; jfr förmedling via Fidonet där uppgifterna "ekas" till ett land som inte anslutit sig till Europarådets dataskyddskonvention. Från Datainspektionens sida har man dock gjort den bedömningen att bestämmelserna om förbud mot utlämnande i praktiken relativt sällan blir tillämpliga på tjänster för förmedling av elektroniska meddelanden.

För den händelse en registrerad tillfogas skada genom att ett personregister innehåller oriktiga eller missvisande uppgifter om honom har den registeransvarige ett strikt skadeståndsansvar (23 § DL). Detta kan, på området för elektroniska förmedlingstjänster leda till synnerligen långtgående förpliktelser, utan motsvarande möjligheter för den registeransvarige att ha kontroll över andras uttalanden m.m.

10.2.4 Arkivering — gallring

Arkivfrågor har behandlats i avsnitt 6.4; se även bilaga 3. Att dokumentera, registrera och redovisa handlingar enligt olika regler i arkivlagen — datalagen och sekretesslagen — kan medföra betydande svårigheter i anknytning till myndigheters användning av elektroniska förmedlingstjänster. Vid uppkoppling respektive nedkoppling av teleförbindelser mellan myndigheter och elektroniska förmedlingstjänster, samt upprättande av elektroniska förmedlingstjänster inom myndigheter respektive nedkoppling av sådana förbindelser, kan således frågor om arkivbildning, arkivvård och gallring aktualiseras.

10.2.5 Sekretess

Bestämmelserna om sekretess och om tystnadsplikt bereder skydd såväl för den enskildes personliga integritet som för det allmännas och företagens intressen av skydd för känsliga uppgifter. Regleringen har visserligen delvis IT-anpassats, men inte för en användning av elektroniska förmedlingstjänster där myndigheter tillhandahåller uppgifter för allmänheten, andra myndigheter eller andra verksamhetsgrenar inom samma myndighet. I princip skall en sekretessprövning äga rum i varje enskilt fall där ett utlämnande aktualiseras, något som knappast

kan förenas med den fria åtkomst och rationella masshantering som en elektronisk förmedlingstjänst syftar till.

När myndigheter tillhandahåller uppgifter via sådana förmedlingstjänster framträder en situation som liknar den vid diarieföring, där det ligger i sakens natur att en sekretessprövning måste göras redan i anslutning till att diarieföringen sker.[21] Inom ramen för de möjligheter till sökningar och sammanställningar som en elektronisk förmedlingstjänst kan erbjuda framträder dock — även om en sekretessprövning föregår införandet vid förmedlingstjänsten — risken för att harmlösa uppgifter sammanställs så att en föreskrift om sekretess blir tillämplig på den nya uppgiftskonstellationen.

Enligt 14 kap. 8 § sekretesslagen kan regeringen dock, förutom när det särskilt anges i bestämmelse om sekretess, för särskilt fall förordna om undantag från sekretess när det är påkallat av synnerliga skäl. Enligt regeringens beslut rörande personregistren i Information Rosenbad, medges att uppgifterna får lämnas ut för automatisk databehandling i utlandet, även i annan stat än sådan som har anslutit sig till Europarådets konvention om skydd för enskilda vid automatisk databehandling av personuppgifter.

De tillämpningssvårigheter som berörts ovan beträffande datalagens bestämmelser om förbud mot visst utlämnande, aktualiseras inom ramen för 7 kap. 16 § sekretesslagen (1980:100) vid utlämnande av personuppgift från en myndighets personregister (jfr 11 § andra stycket DL).

10.2.6 Grundlagsfrågor, m.m.

Yttrandefrihet och nya medier

Den svenska folkstyrelsen bygger enligt 1 kap. 1 § andra stycket regeringsformen (RF) på fri åsiktsbildning och allmän och lika rösträtt. Den fria åsiktsbildningen förutsätter bl.a. yttrandefrihet och informationsfrihet. Dessa friheter, som tillförsäkras medborgarna i 2 kap. 1 § första stycket punkterna 1 och 2 RF, gäller oberoende av vilket medium som används och de får begränsas endast genom lag och endast under vissa förutsättningar som anges i 12 och 13 §§ samma kapitel. Yttrandefriheten har en central ställning genom att den ingår som moment i alla de andra friheter som upptas i 2 kap. 1 § första stycket RF.

Friheten att yttra sig i tryckt skrift regleras närmare i tryckfrihetsförordningen (TF), medan friheten att yttra sig genom ljudradio, television, filmer, videogram, ljudupptagningar m.m. regleras närmare i yttrandefrihetsgrundlagen (YGL). Reglering kompletteras av lagen

[21] Jfr RSV:s handbok Offentligt eller hemligt, s. 38.

(1991:1559) med vissa föreskrifter på TF:s och YGL:s områden, kallad tillämpningslagen.

Sådana interaktiva medier som elektroniska förmedlingstjänster faller i princip utanför TF:s och YGL:s tillämpningsområde. Endast framställningar som är *riktade till allmänheten* innefattas enligt 1 kap. 6 § YGL. Detta krav innebär att en sändning skall riktas till vem som helst som önskar ta emot den, utan särskild begäran från mottagaren. Den som mottar sändningen är aktiv endast genom att slå på mottagaren och välja kanal. När information sänds från en elektronisk förmedlingstjänst tar emellertid mottagaren kontakt med sändaren och väljer vilken information han vill ta del av. En sändning från en sådan tjänst är alltså inte riktad till allmänheten på samma sätt som sändningar av ljudradio och television utan är vad man brukar kalla interaktiv.

Föreskrifterna i YGL om radioprogram tillämpas emellertid också när en redaktion för en tryckt periodisk skrift eller för radioprogram, ett företag för framställning av filmer eller ljudupptagningar eller en nyhetsbyrå med hjälp av elektromagnetiska vågor *på begäran tillhandahåller allmänheten upplysningar* direkt ur ett register med upptagningar för automatisk databehandling (1 kap. 9 § första meningen). Därmed kan YGL bli tillämplig också vid användningen av elektroniska förmedlingstjänster. Detta gäller emellertid inte om den mottagande kan ändra innehållet i registret (1 kap. 9 § andra meningen), och elektroniska förmedlingstjänster som är av intresse från kontrollsynpunkt baseras vanligtvis på en sådan vid interaktivitet.

TF tillämpas också på radioprogram som avses i YGL om ägaren till en periodisk skrift sprider eller låter sprida skriftens innehåll eller delar av detta i form av ett radioprogram, i den utsträckning den i sådan form spridda versionen återger innehållet i skriften oförändrat samt anger hur innehållet har disponerats (1 kap. 7 § andra stycket TF). Enligt 1 kap. 1 § tredje stycket YGL skall vad som sägs i grundlagen om radioprogram gälla också innehållet i vissa sändningar av ljud, bild eller text som sker med hjälp av elektromagnetiska vågor. Enligt lagmotiven avsågs därmed bl.a. videotex.[22] Bestämmelserna torde omfatta endast framställningar som är riktade till allmänheten.

I anknytning till elektroniska förmedlingstjänster kan alltså såväl TF som YGL aktualiseras, men bara vid sändning från en förmedlingstjänst som tillhandahålls av ett massmediaföretag utan att användarna kan ändra innehållet i registret, och — såvitt avser TF — endast om den elektroniskt spridda versionen återger innehållet i skriften oförändrat samt anger hur innehållet har disponerats.

Alla upplysningar som tillhandahålls inom ramen för ett skyddat "radioprogram" *omfattas inte* av grundlagsskyddet. Innebörden av och

[22] Prop. 1990/91:64 s. 108.

syftet med tryck- och yttrandefriheten framgår av 1 kap. 1 § första och andra styckena TF och 1 kap. 1 § första och andra styckena YGL. Där anges att grundlagarna tillförsäkrar medborgarna rätt att i de skyddade medierna offentligen uttrycka tankar, åsikter och känslor och att i övrigt lämna uppgifter i vilket ämne som helst till säkrande av ett fritt meningsutbyte och en fri och allsidig upplysning.[23] En användning av de grundlagsskyddade medierna på ett sätt som inte har med ett fritt meningsutbyte, en fri och allsidig upplysning och ett konstnärligt skapande att göra faller således utanför TF:s och YGL:s skydd. Exempelvis bestraffas bedrägeri som begås genom användning av ett medium som skyddas av TF eller YGL enligt vanlig lag, eftersom bedrägeri inte utgör missbruk av tryck- eller yttrandefriheten såsom den beskrivs i nämnda lagrum. Av samma skäl anses också att reklam i grundlagsskyddade medier i viss mån får regleras genom vanlig lag, utan uttryckligt stöd i TF eller YGL.

Vidare skyddas framställningar endast om de är fixerade i ett medium på sådant sätt att det är möjligt att i förväg bestämma vad som får yttras och att i efterhand fastställa vad som har yttrats. Att dessa möjligheter föreligger är en förutsättning för att ett ensamansvar för vad som yttras i mediet skall kunna gälla. Ett skydd i grundlag för friheten att yttra sig i andra, mindre fixerade former ges endast i regeringsformen.

Bestämmelserna i TF och YGL bygger på principen om *ensamansvar*, dvs. att endast en av de oftast många personer som medverkat vid tillkomsten av en framställning enligt TF eller YGL kan hållas straffrättsligt ansvarig för innehållet i framställningen och att det i dessa grundlagar anges vem denna person är. Vanliga straffrättsliga regler om ansvar för medverkande tillämpas alltså inte. Ansvaret är vidare successivt, dvs. att det i första han åvilar den som står närmast brottet (t.ex. utgivaren av en tryckt periodisk skrift) och om ansvaret inte kan utkrävas av denne vilar det på den som står närmast honom i ansvarskedjan (för en tryckt periodisk skrift ägaren). Slutligen är ansvaret formellt på så sätt att det vilar på den som anges i TF eller YGL, oavsett hur han har bidragit till framställningens tillkomst och oavsett om han har känt till dess innehåll.[24]

I anknytning till elektroniska förmedlingstjänster aktualiseras ett sådant ansvar när ett mediaföretag tillhandahåller upplysningar direkt

[23] I YGL:s ändamålsbestämmelse nämns också ett fritt konstnärligt skapande. Detta har inte ansetts innebära någon skillnad mellan de båda grundlagarnas syften utan har ansetts nödvändigt där på grund av att vissa av de medier som omfattas av YGL har liten betydelse för meningsutbyte och upplysning.

[24] Se beträffande det senare 8 kap. 12 § TF och 6 kap. 7 § YGL. Utgivarens ansvar bortfaller dock om han var utsedd för skens skull eller uppenbarligen inte hade den befogenhet att utöva tillsyn över framställningens offentliggörande och bestämma över dess innehåll som skall tillkomma honom (8 kap. 2 § andra stycket TF och 6 kap. 2 § första stycket andra punkten YGL).

ur ett register utan att mottagaren kan ändra innehållet i registret. Därvid tillämpas bestämmelserna om radioprogram. Sådana program skall ha en utgivare. I första hand ansvarar denne och i andra hand den som bedriver sändningsverksamheten.[25] Detta kan jämföras med reglerna i TF för tryckt periodisk skrift enligt vilka det skall finnas en utgivare som skall anmälas hos Patent- och registreringsverket och som ansvarar för tryckfrihetsbrott. Om ansvar inte kan utkrävas av en utgivare ansvarar skriftens ägare. Därefter följer i ansvarskedjan den som tryckt skriften och utspridaren.[26]

För övriga grundlagsskyddade medier har frågan om ansvar anpassats på annat sätt till respektive mediums särart. Beträffande t.ex. tryckfrihetsbrott genom en skrift som inte är periodisk vilar ansvaret i första hand på författaren, om han framträtt frivilligt. De följande stegen i ansvarskedjan är förläggaren, tryckaren och spridaren.[27] Beträffande ljudupptagningar ges enligt YGL en möjlighet att välja om utgivare skall utses eftersom produktionen av ljudupptagningar i många fall inte kan föranleda straff- eller skadeståndsansvar.[28]

Av intresse i sammanhanget är vidare principen om källskydd, som innefattar bl.a. en rätt till anonymitet, tystnadsplikt beträffande vissa personers identitet, ett förbud för myndigheter och andra allmänna organ att forska efter uppgiftslämnare etc., samt rätten för envar att anskaffa uppgifter för offentliggörande.

Offentlighetsprincipen och registreringsskyldigheten enligt sekretesslagen

Frågan om tillämpning av bestämmelserna om offentlighetsinsyn och registreringsskyldighet enligt sekretesslagen på upptagningar som görs tillgängliga via nät har redan behandlats i avsnitt 6.1. Med den tolkning jag har förordat av 2 kap. 6 § första stycket andra meningen TF torde det inte föreligga några hinder i det avseendet mot att myndigheter bereds tillgång till elektroniska förmedlingstjänster.

I det föregående har emellertid inte berörts de rättsfrågor som uppkommer när en tjänsteman tar del av meddelanden vid en elektronisk förmedlingstjänst eller sänder meddelanden till en sådan tjänst. Elektroniska meddelanden kan mer eller mindre påtagligt knytas till en tjänstemans aktiviteter genom att han tar del av meddelanden vid någon förmedlingstjänst. Han kan därvid inskränka sig till att läsa eller annars

[25] 4 kap. 1 § första stycket och 6 kap. 1 och 2 §§ YGL, se 3 kap. 1 och 3-18 §§ tillämpningslagen om anteckning och anmälan av utgivare.

[26] Se 5 kap. 2 och 4 §§ samt 8 kap. 1-4 och 10-12 §§ TF och 2 kap. 2 § tillämpningslagen.

[27] Se 8 kap. 5-9 och 10-12 §§ TF, där särskild reglering ges för samlingsverk och verk av en avliden författare.

[28] Se 4 kap. 7 § YGL och 4 kap. 1 § tillämpningslagen.

ta del av vissa meddelanden via bildskärm, men det finns vanligtvis inga hinder mot att skriva ut dem eller lagra dem elektroniskt hos myndigheten. När tjänstemannen sänder elektroniska meddelanden går tanken till expediering av handlingar.

De grundläggande synsätten bakom definitionerna i TF av en förvarad och inkommen eller upprättad handling har visat sig bli allt svårare att överföra till kommunikation via nät, där meddelandena skall bedömas utifrån såväl TF:s som sekretesslagens, arkivlagens och förvaltningslagens synsätt.

11 Överväganden

11.1 Utgångspunkter

Tjänster för förmedling av elektroniska meddelanden spelar en viktig roll, bl.a. som medium för ett fritt meningsutbyte, en fri och allsidig upplysning och ett fritt konstnärligt skapande. Internet och andra interaktiva tjänster erbjuder en mångfald av politisk diskussion och ett kulturellt utbyte över nästan alla gränser. Utvecklingen har skett på kort tid och med ett minimum av statlig inblandning och reglering.

I Sverige finns ingen lagstiftning som tar sikte på sådana förmedlingstjänster och de bestämmelser som aktualiseras är baserade på en datoranvändning som förekom på 1960- och 1970-talen. Detta regelverk fungerar inte i den nya miljön och det är delvis oklart hur bestämmelserna bör tolkas. Vissa föreskrifter efterlevs inte medan andra tolkas så att de kan förenas med de nya formerna för kommunikation.[1]

För att bevara och förstärka en dynamisk utveckling är det angeläget att undanröja hinder mot ett fritt meningsutbyte. Samtidigt behöver intresset av att bekämpa brottslig eller annars oacceptabel spridning av information beaktas. Som jag konstaterat i avsnitt 10.2.1 och 10.2.2 är detta dock till stor del möjligt redan inom ramen för gällande straff- och processrättsliga reglering, och det bör på detta stadium införas så få nya regler som möjligt. Risken är uppenbar att ett alltför omfattande regelverk snabbt skulle föråldras och hindra en positiv utveckling på området. Sådana synpunkter framfördes också när utredningen, som berörts i kapitel 1, under augusti 1995 spred en promemoria med förslag till reglering på området och med denna som underlag höll en hearing med tekniker och administratörer samt en hearing med jurister. Jag har tagit intryck av den kritik som då framfördes och sökt begränsa förslagets omfattning samt beakta behovet av att de begrepp m.m. som används görs teknikneutrala.

[1] Sådana exempel kan hämtas från datalagen (1973:289), som jag återkommer till i det följande.

I det följande behandlas först anpassningar för att undanröja hinder mot ett fritt meningsutbyte och därefter skyddet mot missbruk av elektroniska förmedlingstjänster.

11.2 Anpassningar för att undanröja hinder mot ett fritt meningsutbyte

11.2.1 Skyddet för persondata

De hinder som kan uppkomma mot ett fritt meningsutbyte via elektroniska anslagstavlor och liknande förmedlingstjänster har samband med EG-direktivet om persondataskydd (dataskyddsdirektivet) och regleringen i datalagen (DL). Dessa bestämmelser har inte utformats med sikte på en sådan IT-användning som förekommer i anknytning till elektroniska förmedlingstjänster.

Inläggen i t.ex. en debatt vid en elektronisk förmedlingstjänst kan — beroende på ändamålet med databehandlingen — bli att bedöma som personregister (1 § DL) och innehålla bl.a. sådana värderingar och omdömen att registret, utöver licens, kräver tillstånd av Datainspektionen (2 § DL). Vidare aktualiseras frågor om utlämnande, rättelse, ändring, uteslutning, komplettering och gallring av personuppgifter, utdrag enligt 10 § DL, förteckning över personregister och skadeståndsansvar; jfr avsnitten 6.3 och 10.2.3.

Till detta kommer Sveriges åtaganden enligt dataskyddsdirektivet. Direktivet är tillämpligt på all IT-baserad behandling av personuppgifter och ställer upp stränga krav för behandling av sådana uppgifter. Det krävs omfattande avsteg från huvudreglerna i dataskyddsdirektivet för att tillgodose intresset av yttrande- och informationsfrihet vid elektroniska förmedlingstjänster. Direktivets definition av personuppgifter innehåller inget rekvisit som tar sikte på om en uppgift skall användas för att identifiera någon individ och det finns inga undantag för löpande text.

DL är, enligt Datainspektionens praxis, bara i undantagsfall tillämplig på löpande text vid elektroniska förmedlingstjänster. Lagen anses gälla endast om syftet är att återsöka och sammanställa uppgifter om personer som kan finnas angivna i de elektroniska meddelandena. Från Datainspektionens sida har man gjort den bedömningen att en sådan användning av förmedlingstjänster som innebär att löpande text utgör personregister till och med är så ovanlig att det inte behövs något undantag från DL för löpande text, och det har gjorts gällande att DL även fortsättningsvis bör tillämpas på register över användare etc.

De sökverktyg m.m. som tillhandahålls vid elektroniska förmedlingstjänster möjliggör vanligtvis återsökning och sammanställning av uppgifter om fysiska personer, och tjänsterna fungerar ofta så att den

som tillhandahåller dem inte styr och inte närmare vet för vilka ändamål de kommer att användas. Förutsättningarna avviker härvid i sådan mån från de tillämpningar för vilka DL och dataskyddsdirektivet är skrivna att jag föreslår en självständig reglering för elektroniska förmedlingstjänster, som i denna del syftar till att skapa en frizon för ett fritt meningsutbyte.[2] Enligt min mening bör därvid ett undantag från DL föreskrivas för löpande text, särskilt som vissa ifrågasätter Datainspektionens tolkning. Ett uttryckligt undantag är bättre än ett underförstått, och det kan inte bortses från att gränsfall annars framträder som är svåra att komma till rätta med för den som ansvarar för en elektronisk förmedlingstjänst.

Valet av lagteknisk lösning sammanhänger också med att DL inom kort kan antas bli ersatt av en moderniserad reglering, anpassad till dataskyddsdirektivet. Det är inte lämpligt att kort tid dessförinnan införa en ny reglering som tar sin utgångspunkt i DL.

11.2.2 Undantag för löpande text, m.m.

Jag har som sagt kommit fram till att det, för de elektroniska förmedlingstjänsternas del, bör göras ett undantag från DL för *löpande text*. Jag återkommer nedan till den närmare innebörden i detta begrepp och en begränsning av undantaget.

I den mån *egentliga register* förekommer vid en elektronisk förmedlingstjänst bör DL emellertid gälla även i fortsättningen, med undantag för sådana register över användare och elektroniska meddelanden som förs vid förmedlingstjänsterna och som behövs för att användarna skall kunna hämta och lämna meddelanden. Användarna har vanligtvis själva tillfört dessa uppgifter, och registren kan knappast — om de begränsas till sådana uppgifter som krävs för hanteringen av förmedlingstjänsten — medföra risker för otillbörligt integritetsintrång. Därför bör också användarregister, diarier och liknande sammanställningar samt sådana "menyer" som förekommer för att sortera och strukturera elektroniska meddelanden undantas från DL:s tillämpningsområde.

Genom en sådan indelning blir det avgörande för frizonens omfattning hur begreppet löpande text bör förstås. Denna fråga har aktualiserats bl.a. i anknytning till *DL:s personregisterbegrepp*. Enligt lagmotiven anses ett ADB-register inte vara upprättat bara genom att *löpande text* lagras, t.ex. för tryckning, utan först om databehandlingen tar sikte på faktiska uppgifter i den litterära framställningen.[3] Vidare

[2] Utrymmet för fritt meningsutbyte via elektroniska förmedlingstjänster avgörs av hur omfattande undantag som kan göras, samtidigt som Sveriges åtaganden enligt direktivet begränsar handlingsutrymmet.

[3] Prop. 1973:33 s. 118 f.

bör man enligt kommentaren till DL i många fall se som personregister en sådan ADB-användning som brukas som hjälpmedel vid författande, lagring, överföring och utskrift av brev och andra dokument, förutsatt att t.ex. namn eller personnummer används som sorterings- eller sökbegrepp.[4] Den närmare gränsdragningen får enligt motiven göras i praxis. Rättsläget är oklart.

Enligt min mening behöver en reglering av elektroniska förmedlingstjänster ges klara gränser som enkelt kan förstås av t.ex. användare och dem som är ansvariga för förmedlingstjänster. Den närmare innebörden av begreppet "löpande text" bör därför knyta an till allmänt språkbruk, dvs. till *den faktiska utformningen* av en text. Genom en sådan inriktning kan subtila gränsdragningar som följer av att regleringen tar sin utgångspunkt i vissa ändamål med databehandlingen undvikas.

Med löpande text bör således förstås sådan vanlig fri text som inte har en struktur som gör det enkelt att automatiskt sammanställa och bearbeta många uppgifter om en viss person eller en viss typ av uppgifter om många personer. Även om sådan löpande text kan databehandlas med sikte på personuppgifter, t.ex. genom att använda ett namn som sökbegrepp, utgör texten inte ett egentligt register eftersom den inte har strukturerats så att sökning av personuppgifter underlättas. Det behövs människor för att tolka en sådan text. Detsamma gäller datorprogram och digitala bilder, såvida inte särskilda åtgärder har vidtagits.

Däremot bör text som är förberedd för att enkelt kunna omvandlas till en strukturerad form eller annars användas som om den vore strukturerad inte falla inom ramen för det begrepp löpande text som jag föreslår. Som exempel kan nämnas att ett egentligt register kan konverteras till något som ser ut som vanlig text. Ett annat exempel är om några användare, med stöd av en elektronisk konferens, kontrollerar vissa personer genom att — så snart en iakttagelse gjorts rörande en viss person — föra in detta som ett meddelande i konferensen med den iakttagna personens namn som ärendemening. Användarna kan utnyttja denna struktur genom att söka i ärendemeningarna och på så sätt snabbt få besked om vad som har rapporterats beträffande en viss person. Även andra åtgärder varigenom löpande text strukturera s så att personuppgifter skall kunna sammanställas eller tolkas automatiskt av ett datorprogram bör anses medföra att ett egentligt register föreligger.[5]

[4] Kring/Wahlqvist, Datalagen, 1989, s. 56. Den bedömning som gjorts rörande bildfångade (scannade) pappershandlingar inom skatteförvaltningen kan förenas med detta resonemang. Handlingarna, som är sökbara endast i ett särskilt register med t.ex. den skattskyldiges personnummer och namn, ses som delar i skattemyndigheternas personregister (Ds 1994:80 s. 124 och prop. 1994/95:93).

[5] Sådan struktur föreligger vid t.ex. Electronic Data Interchange (EDI), som syftar till att datorer skall kunna "tolka" inkomna meddelanden och "agera" utifrån dem.

Denna bedömning framstår som självklar om strukturen medger att frågor ställs av typen: räkna upp namnen på de som är registrerade och har mer än tre barn, har högre lön än 150 000 kr etc., eller förteckna vid vilka tidpunkter och platser en person har företagit en viss åtgärd, t.ex. använt sitt kreditkort. Detsamma bör emellertid gälla när strukturen avser personuppgifter som uppfattas som ointressanta från integritetssynpunkt. En reglering som baseras på bedömningar av skyddsbehovet i stället för materialets struktur blir alltför komplicerad för att passa på området för elektroniska förmedlingstjänster.

Sökmöjligheter med inriktning på strukturer av beskrivet slag förekommer emellertid knappast vid elektroniska förmedlingstjänster och de möjligheter att söka på fri text som brukar ges fråntar inte materialet karaktären av löpande text. Bland de gränsfall som i praktiken kan aktualiseras bör nämnas litteraturförteckningar och liknande material med personuppgifter som knyts till annan text som sprids via en elektronisk förmedlingstjänst. Sambandet med den löpande texten är i dessa fall sådant att uppgifterna redan enligt vanligt språkbruk uppfattas som en del av den fria texten. Det går emellertid inte att helt undgå ett gränsområde där strukturen når en sådan grad att det kan ifrågasättas om ett egentligt register föreligger.

Jag föreslår alltså att de elektroniska förmedlingstjänsterna undantas från DL i den mån de register som förs där bara innehåller löpande text — dvs. sådana meddelanden som inte har strukturerats så att sökning av personuppgifter underlättas — och uppgifter om meddelanden och användare.

Syftet med ett sådant undantag från DL är att främja ett fritt meningsutbyte, en fri och allsidig upplysning och ett fritt konstnärligt skapande, dvs. de intressen som skyddas av yttrandefrihetsgrundlagen. Undantaget bör därför begränsas till sådana elektroniska förmedlingstjänster som drivs i dessa syften. Detta bör gälla såväl för löpande text som för uppgifterna om användare och meddelanden.

När datorer och telekommunikationer används för andra syften bör DL således tillämpas på vanligt sätt i den mån det förekommer personregister. Som framgått bör DL också tillämpas vid elektroniska förmedlingstjänster som har ett yttrandefrihetsrättsligt syfte, i den mån det förekommer andra egentliga personregister än register som innehåller uppgifter om användare och meddelanden.

Bestämmelserna i 21 § DL om dataintrång är inte begränsade till personregister.[6] Undantaget från DL skall naturligtvis inte omfatta denna straffbestämmelse. Bestämmelserna i 26-28 §§ DL om det statliga person- och adressregistret SPAR bör inte heller undantas. Om den situationen skulle uppkomma att någon begär att — ur en myndig-

[6] Datastraffrättsutredningen har föreslagit att dessa bestämmelser skall föras in i brottsbalken, i de sammanhang där de hör hemma.

hets personregister — få uppgifter som avses i 26 § andra stycket 1 och 3 DL, och registret är knutet till en elektronisk förmedlingstjänst, bör en hänvisning enligt 28 § första stycket DL till SPAR alltjämt vara möjlig. Jag föreslår alltså ett undantag från DL som omfattar 1-20 och 22-25 §§ DL.

Registeransvaret enligt DL har, som framgått av avsnitt 10.2.3, utformats så att det möjligen skulle kunna ifrågasättas om varje användare av en elektronisk förmedlingstjänst blir att bedöma som registeransvarig. Jag har därför övervägt en uttrycklig föreskrift om att den som använder tjänsten inte är registeransvarig. Det torde emellertid vara så osannolikt att elektroniska förmedlingstjänster skulle anses vara förda för användarnas verksamhet att en sådan bestämmelse kan undvaras.

Som närmare behandlas i avsnitt 11.3 föreslår jag en särskild lag om elektroniska förmedlingstjänster, där undantagen från DL bör föras in. Vidare bör en hänvisning till dessa bestämmelser ges i DL (2 § förslaget till lag om elektroniska förmedlingstjänster och 1 a § förslaget till lag om ändring i datalagen).

11.2.3 Förhållandet till dataskyddsdirektivet

Spänningen mellan behovet av att säkerställa yttrande- och informationsfriheten respektive att motverka otillbörligt integritetsintrång framträder i ännu högre grad i anknytning till EG-direktivet om persondataskydd.

De krav på skydd för den enskilde som ställs upp i direktivet går längre än regleringen i DL. Dessutom är direktivets tillämpningsområde vidare. All löpande text där personuppgifter databehandlas omfattas av direktivet och den registeransvarige åläggs bl.a. omfattande administrativa skyldigheter, som knappast kan förenas med ett fritt informationsflöde vid elektroniska förmedlingstjänster. En undantagslös tillämpning av direktivets huvudprinciper torde i praktiken sätta stopp för detta medium i omodererad form.

Enligt artikel 9 skall medlemsländerna emellertid, beträffande behandling av personuppgifter som sker för journalistiska ändamål eller konstnärligt eller litterärt skapande, besluta om de undantag och avvikelser som visar sig nödvändiga för att förena rätten till privatlivet med reglerna om yttrandefriheten. I direktivets inledning uttalas också att direktivet gör det möjligt att vid genomförandet ta hänsyn till principen om allmänhetens rätt till tillgång till allmänna handlingar.

En omständighet av betydelse när det gäller att bedöma hur omfattande undantag som kan och bör göras med stöd av artikel 9 är den avgränsning som i direktivet görs med avseende på manuell behandling av personuppgifter. Direktivet är tillämpligt dels på automatisk behandling av personuppgifter, dels på *manuell* behandling som är

strukturerad så att sökning av personuppgifter underlättas. Om en sådan struktur saknas, är direktivet inte tillämpligt. Skälet är uppenbarligen att manuell löpande text är mindre känslig än egentliga (manuella) register. — Det kan också noteras att förekomsten av elektroniska förmedlingstjänster inte nämns i direktivet.

Vid en reglering av de elektroniska förmedlingstjänsterna är det enligt min mening naturligt att utgå från direktivets principiella ställningstagande, att det skall vara möjligt att förena rätten till privatlivet med yttrandefriheten och ta hänsyn till allmänhetens rätt till tillgång till allmänna handlingar. Regleringen måste stå i samklang med vår starka tradition att — oberoende av medium — bereda skydd för yttrande- och informationsfriheten i vid mening.

Som framgått föreslår jag att ett undantag från DL (och därmed också från en reviderad datalag som tar hänsyn till direktivet) skall göras bara för löpande text och uppgifter om meddelanden och användare, samt endast under förutsättning att den elektroniska förmedlingstjänsten drivs enligt de principer som skyddas av yttrandefrihetsgrundlagen. Mot den bakgrund som jag har redovisat ovan måste dessa avsteg från direktivets huvudregler anses vara förenliga med våra förpliktelser som medlem i Europeiska unionen.

11.2.4 Personligt bruk

Med det system jag föreslår kommer det att vid en elektronisk förmedlingstjänst kunna förekomma även andra egentliga register än registren över användare och meddelanden, förutsatt att förandet av registret inte står i strid med DL. En särskild fråga som då inställer sig är, om ett sådant register skall kunna anses vara inrättat eller fört *uteslutande för personligt bruk* och därför enligt 2 § tredje stycket DL falla utanför licens- och tillståndsplikten.

Motiven till bestämmelsen[7] är inriktade på frågan om vad som är näringsverksamhet, dvs. graden av användning i eller i anknytning till förvärvsverksamhet. I underrättspraxis har undantaget ansetts tillämpligt på en elektronisk förmedlingstjänst som hållits tillgänglig för en obestämd krets personer (som mest 1 200 registrerade användare); det ansågs inte framgå att lagstiftarens avsikt varit att undantaget från licenstvång skulle avse endast *eget* personligt bruk.[8]

Lagtextens ordalydelse ("uteslutande för personligt bruk") gör det emellertid svårt att förena detta undantag med en registeranvändning vid en elektronisk förmedlingstjänst, särskilt när sådana förmedlingstjänster nu görs till föremål för en offentligrättslig reglering. En tolkning som innebär att tillhandahållande av personregister via en

[7] Se bl.a. prop. 1981/82:189 s. 54 f. och SOU 1990:61 s. 160.
[8] Sundsvalls tingsrätts dom den 2 november 1993, DB 728.

elektronisk förmedlingstjänst inte kan vara personligt bruk enligt 2 § tredje stycket DL är också förenlig med Datainspektionens praxis och det synsätt som framträder när bestämmelsen sätts in i sitt sammanhang; det är inte rimligt att bedöma behovet av licens eller tillstånd som mindre uttalat på ett område där det föreligger uppenbara risker för en omfattande spridning av känsliga personuppgifter.

Enligt min mening behövs det alltså ingen författningsändring för att klargöra att undantaget i 2 § tredje stycket DL inte är tillämpligt när databaser görs allmänt tillgängliga via en elektronisk förmedlingstjänst som omfattas av den reglering jag föreslår.

11.3 Regler till skydd mot missbruk

11.3.1 Bör en särskild reglering införas?

Utvecklingen av telekommunikationer och anknytande tjänster går mycket fort samtidigt som missbruket av dessa tjänster ständigt tar sig nya uttryck. När utredningens direktiv skrevs framstod elektroniska anslagstavlor som objektet för eventuella åtgärder, dvs. sådana anslagstavlor som användarna når genom att med modem ringa ett visst (svenskt) abonnentnummer till vilket en dator där tjänsten tillhandahålls är ansluten. Där finns visserligen ofta även utländskt material, men detta har då kopierats ("ekats") till datorer i Sverige.

Den explosionsartade utvecklingen av informationstjänster knutna till bl.a. det världsomspännande nätet Internet har komplicerat bilden. Internet kan nås med hög överföringskapacitet och överföringen sker till allt lägre kostnader. Elektroniska meddelanden kopieras därför vanligtvis inte till en mängd datorer. I stället hämtar användarna data där de ursprungligen har lagrats — delvis oberoende av i vilka länder användarna och de elektroniska påfarterna till näten finns. Därmed har den fysiska knytningen av en viss verksamhet till ett visst lands territorium begränsats.

Här är utvecklingen på det radiorättsliga området av intresse.[9] I och med att sändningar av TV-program via satellit blev vanliga raserades grunden för dåvarande reglering på området. Det fanns röster som förordade förbud mot användning av paraboler i Sverige. Frågan löstes emellertid genom den europeiska konventionen om gränsöverskridande television, enligt vilken sändarlandet skall se till att sändningarna uppfyller vissa minimikrav. Om de gör det är övriga länder skyldiga att inte hindra mottagning av dem. Motsvarande regler finns nu inom EU

[9] Ursprungligen fanns endast en TV-kanal i Sverige och den kunde enkelt regleras med hänsyn till bl.a. verksamhetsform. Situationen komplicerades påtagligt i och med att ytterligare kanaler, bl.a. lokala sändningar, tillkom. En nationell reglering var dock alltjämt möjlig.

(det s.k. TV-direktivet). Det kan alltså invändas att en nationell reglering på det område mitt uppdrag avser inte skulle vara meningsfull eller ens önskvärd eftersom verksamheter kan flytta från Sverige och alltjämt erbjuda svenska användare tillgång till samma information (jfr prop. 1995/96:125 s. 22).[10]

Verksamheter kan emellertid antas komma att bedrivas elektroniskt via nät i en ökande takt, och det kan inte accepteras att svenskt territorium blir en elektronisk tummelplats för otillåten spridning av information m.m. Den tilltagande globaliseringen kan alltså inte utgöra skäl att avstå från en reglering som från andra utgångspunkter kan te sig angelägen, och det bör inte bortses från att det — enligt de uppgifter jag har fått — alltjämt torde vara så att verksamheter direkt inriktade på brott bedrivs i Sverige genom elektroniska anslagstavlor som inte är knutna till Internet eller andra sådana globala nät för datorkommunikation. Enligt min mening är det visserligen i första hand genom internationella överenskommelser som man bör söka komma till rätta med missbruk och avarter, och det är en angelägen uppgift att från svensk sida verka för att sådana överenskommelser kommer till stånd. Man får emellertid räkna med att det tar tid innan en sådan inriktning ger resultat. Det måste därför övervägas om man bör införa särskilda regler till skydd mot missbruk av elektroniska förmedlingstjänster och hur en särreglering kan motiveras.

De straffrättsliga och straffprocessuella frågor som härvid aktualiseras är allmängiltiga och kan antas i någon mån bli aktuella vid varje förundersökning i IT-miljö. En genomlysning av området har gjorts av Datastraffrättsutredningen, och Sverige har nyligen antagit Europarådets rekommendation No. R (95) 13 angående straffprocessuella frågor med anknytning till IT, där författningsändringar för att möjliggöra eller förenkla utredningar av brott i IT-miljö förordas. Enligt min mening är det angeläget att en sådan översyn görs. Möjligheterna att förebygga och utreda brott i anknytning till tjänster för förmedling av elektroniska meddelanden behöver förbättras.

Frågan är emellertid om härutöver en särreglering rörande tjänster för förmedling av elektroniska meddelanden bör införas. Ett skäl för en särskild reglering är — som tidigare berörts — behovet av att undanröja de enligt min mening onödiga hinder mot ett fritt meningsutbyte som nuvarande lagstiftning ställer upp. Det missbruk som enligt det

[10] Som exempel kan nämnas att det, sedan en amerikansk domstol dömt till fängelse för spridning av pornografi mellan två delstater, nu finns en dator i Sverige som har inriktats på att i USA tillhandahålla samma tjänst. Förfarandet torde inte strida mot svensk lag. Frågan brukar populärt sägas röra vem som har jurisdiktion över "cyberspace". De förhållanden som vanligtvis ger praktiska förutsättningar för myndigheter att ingripa mot otillåtna förfaranden och för enskilda att utkräva sin rätt, nämligen att personer och den utrustning som är berörd befinner sig inom landet, föreligger alltså inte vid kommunikation via globala nät. Det torde utgöra ett intrång i främmande lands suveränitet om svenska myndigheter utan medgivande vidtar åtgärder via nät i ett annat land.

föregående förekommer utgör vidare skäl för att ställa upp vissa regler av annan karaktär, som ger struktur och en viss kontroll av de elektroniska förmedlingstjänsterna.

Det kan synas naturligt att här göra jämförelser mellan tjänster för förmedling av elektroniska meddelanden och traditionella telefonsamtal, brev och massmedier av olika slag. Jag har emellertid funnit att sådana jämförelser ofta inte blir särskilt träffande om de förs för långt eftersom IT-användningen effektivt bryter igenom gränserna mellan traditionella medier och tillämpningar. Ena stunden kan den elektroniska tjänsten användas t.ex. som radio eller TV, medan den i nästa ögonblick kan brukas för att bl.a. distribuera post eller föra samtal i realtid. — Jag återkommer dock i avsnitt 11.3.3 till vissa paralleller som kan dras.

En reglering för att stävja missbruk av elektroniska förmedlingstjänster måste alltså grundas på mer självständiga överväganden. Regleringen kan enligt min mening grundas på tre analogier från straffrätten. Den första utgår från de funktioner en ansvarig utgivare för en tidning fyller och det ansvar han har. En sådan jämförelse förutsätter emellertid att en förhandskontroll kan ske, något som vanligtvis inte är möjligt beträffande sådana tjänster för förmedling av elektroniska meddelanden där missbruk förekommer. Den andra analogin hänger samman med de krav som ställs på medborgarna att förhindra och att avslöja brott samt att aktivt medverka inom ramen för en förundersökning. Kraven på aktiv medverkan är dock begränsade[11] och skyldigheten att förhindra och avslöja brott gäller endast beträffande de grövsta brotten, vilka vanligtvis inte är aktuella i detta sammanhang. Den tredje analogin avser de s.k. oäkta underlåtenhetsbrotten[12], och även denna analogi haltar.

Enligt min mening ger dessa tre analogier dock — trots att de haltar — tillräckligt stöd för att införa en sådan reglering som enligt det föregående är angelägen för att komma till rätta med det missbruk som förekommer. Regleringen behövs för att bygga upp och stärka ett rättsmedvetande på området, bl.a. eftersom det saknas historia och tradition rörande vad som är godtagbart. Detta kan visserligen också ske genom etiska regler, villkor för anslutning till tjänster etc. Sådana åtgärder behöver emellertid stödjas av författningsregleringen och det bör uppmärksammas att vi befinner oss i början av en teknisk utveckling som kan komma att leda till förstärkningar av effekterna av vad som i dag till viss del kan ses som relativt harmlösa former av nätmissbruk (jfr den inverkan bilens genombrott fick för t.ex. kommunikationerna och strafflagstiftningen). Den integration av medier som

[11] Nya straffprocessuella regler om aktiv medverkan har föreslagits av Datastraffrättsutredningen och i den nämnda rekommendationen från Europarådet.

[12] Denna kategori kan här förenklat beskrivas så att överträdelsen består i att någon gör något genom att underlåta att göra något annat, jfr som exempel att döda ett barn genom att underlåta att ge det mat.

nu har inletts kan antas komma att accelerera, och kan föra med sig förändringar i fler avseenden än vi för närvarande kan överblicka. Det blir därmed delvis osäkert vilka personer och företeelser som i praktiken kan komma att omfattas av en reglering. Vid sådana förhållanden måste regleringen — åtminstone inledningsvis — rimligen ges en relativt "mjuk" utformning.

11.3.2 Vilka tjänster bör omfattas av en reglering?

Frågan är då vad som bör ses som objekt för en sådan reglering. Som framgått av avsnitt 10.1.3 finns det många olika slag av elektroniska förmedlingstjänster. Ibland används beteckningen elektronisk anslagstavla eller BBS även med avseende på databaser anslutna till t.ex. Internet och de tjänster som där erbjuds. Det är emellertid knappast möjligt att med en enda term entydigt avgränsa dessa företeelser. Skillnaderna mellan dem har blivit så stora att det till och med har blivit svårt att beskriva dem samlat, inte minst på grund av den höga förändringstakten. Programvaror avsedda för den som är ansluten till Internet ger möjlighet att t.ex. telefonera, lyssna på radio, se på TV och läsa eller hämta elektroniska tidningar eller annan information. Vidare finns de sedvanliga funktionerna för bl.a. e-post och elektroniska konferenser.[13]

Naturligtvis bör det inte införas någon särreglering för enskilda tillämpningar inom ramen för elektroniska förmedlingstjänster såsom radio, TV eller e-post, där den tjänst som tillhandahålls — om man bortser från distributionssättet — är i det närmaste identisk med den traditionella tjänsten.[14] Sådana särregler skulle dessutom bli svåra att utforma eftersom digitaliseringen innebär att gränserna mellan de olika tillämpningarna bryts igenom.

En reglering med sikte på de företeelser som mitt uppdrag avser kan alltså knappast utformas så att vissa tydligt avgränsade medieföreteelser eller vissa tekniska lösningar pekas ut. En sådan lagteknik baserad på en eller flera konkreta tillämpningar skulle förmodligen lätt kringgås genom modifieringar av programvaror så att tjänsterna ges en delvis annan utformning; jfr att World-Wide Web vuxit fram på bara något år.[15] Den enda tydliga och bestående avgränsning av dessa företeelser är alltså, såvitt jag har kunnat finna, att de avser förmedling av

[13] Exempelvis kan den senaste versionen av datorprogrammet Netscape, utöver vanlig åtkomst till World-Wide Web, användas för e-post och elektroniska diskussionsgrupper.

[14] En annan sak är att den som tillhandahåller tjänster via nät kan behöva överväga om t.ex. den radiorättsliga regleringen kan bli tillämplig på hans tjänst.

[15] Från traditionell miljö kan nämnas de svårigheter som uppkommit att ange vad som är narkotika i narkotikabrottslagens mening när mindre kemiska förändringar enkelt kan göras.

elektroniska meddelanden.[16] Med meddelanden avser jag då alla olika former av text, bild, ljud eller information i övrigt som förmedlas i elektronisk form.

En reglering av det område mitt uppdrag avser bör alltså i princip omfatta alla tjänster för extern förmedling av elektroniska meddelanden; se vidare avsnitt 11.4.2.

11.3.3 Vem bör en reglering riktas mot?

Ansvaret för brott och skadeståndsgrundande handlingar m.m. bör självfallet i första hand bäras av den som utför eller ligger bakom den ansvarsgrundande åtgärden, t.ex. den som sänder ett elektroniskt meddelande med information som inte får spridas. Vid användningen av tjänster för förmedling av elektroniska meddelanden kompliceras bilden emellertid av att det kan vara i det närmaste omöjligt att spåra denne, om inte åtgärder vidtas.

Detta kan jämföras med regleringen i TF och YGL, som kan ses som en privilegielagstiftning med särskilda skyddsregler för vissa former av informationsspridning. En förutsättning har här ansetts vara att utredning och beivrande av tryck- och yttrandefrihetsbrott kan ske snabbt och effektivt, utan omfattande utredningar av t.ex. vem som ansvarar för visst material på en stor tidningsredaktion. Därför pekas en viss ansvarig ut — lagstiftaren har här så att säga slagit hål på uppsåtsläran — och det finns bestämmelser om bl.a. bevarande och tillhandahållande av det offentliggjorda materialet. En sådan reglering har setts som ett villkor för en omfattande yttrandefrihet i massmedier, och regleringen gäller bl.a. för tryckt skrift, film, radio och vissa ADB-upptagningar. Den i IT-sammanhang vanliga invändningen, att en ansvarig inte bör pekas ut eftersom denne ofta inte kan överblicka de informationsmängder han skulle komma att svara för, rör därmed inte någon helt ny fråga. Det är naturligtvis svårt för en ansvarig utgivare av en dagstidning att hinna läsa varje artikel och annons.

En jämförelse med en teleoperatör enligt telelagen (1993:597) är också av intresse. Den som driver televerksamhet av viss omfattning har — utöver en tillståndsplikt — ålagts vissa skyldigheter. Han skall bl.a. bedriva verksamheten i enlighet med de villkor som föreskrivs i tillståndet och på begäran lämna t.ex. uppgifter som angår misstanke om brott.

Den som tillhandahåller sådana elektroniska förmedlingstjänster som mitt uppdrag rör får motsvarande nyckelposition. Eftersom han kan bestämma om tjänstens användning, inklusive utformningen av de

[16] Önskan att sätta en enda beteckning på de aktuella företeelserna är alltså inte realistisk och analogier med gällande regler visar sig ofta oförenliga med vissa av de användningssätt som aktualiseras.

tekniska och administrativa rutinerna, blir de val han gör avgörande för vilket utrymme som ges för missbruk och för att spåra den som har missbrukat tjänsten. Jag föreslår därför en reglering med sikte på den som tillhandahåller en elektronisk förmedlingstjänst. Det är denne som kan bestämma hur tjänsten skall användas och som ytterst har den operativa kontrollen över denna. Därigenom blir det möjligt att uppställa sådana krav på verksamheten att den kan överblickas och hanteras av såväl den som tillhandahåller tjänsten som av myndigheter m.fl.

11.3.4 Lagstiftningstekniken

De rättsfrågor som aktualiseras i anknytning till elektroniska förmedlingstjänster spänner över flera regelkomplex och är — om de begränsas till sådana tjänster — inte enkla att passa in i de vedertagna regelmönstren. Vissa rättsfrågor med anknytning till sådana tjänster rör som redan framgått skyddet för persondata: Elektroniska meddelanden innehåller ofta personuppgifter och ett meddelande eller en konferens till vilken meddelandet dirigeras kan — beroende på ändamålet med databehandlingen — bli att anse som ett personregister i DL:s mening. Till en tjänst som avser förmedling av elektroniska meddelanden sänds emellertid främst meddelanden som inte utgör personregister och tjänsten kan bestå enbart av meddelanden som faller utanför personregisterbegreppet. Men även meddelanden som faller utanför DL:s tillämpningsområde kan innehålla t.ex. rasistiska uttalanden, uppmaningar till brott, recept för tillverkning av narkotika m.m.

Eftersom en reglering av elektroniska anslagstavlor och liknande tjänster bör omfatta både sådana meddelanden som i dag omfattas av DL och sådana meddelanden som inte gör det kan regleringen inte gärna tas in i DL.

Bestämmelserna bör inte heller placeras i brottsbalken eller rättegångsbalken eftersom behovet av normgivning är vidare än vad som ryms inom ramen för en renodlad straffrättslig och straffprocessuell reglering.

Möjligen kunde dessa rättsfrågor anses ha ett sådant samband med regleringen av telekommunikationer att bestämmelser om tjänster som avser förmedling av elektroniska meddelanden kunde arbetas in i telelagen; jfr avsnitt 11.6. De skillnader som jag föreslår beträffande tillämpningsområde, inriktning, regelstruktur etc. är emellertid sådana att en särskild lag är lämpligare för den nya regleringen. Jag föreslår därför en lag om elektroniska förmedlingstjänster.

11.3.5 Närmare om den särskilda lagens tillämpningsområde

I dag finns ett mycket stort antal elektroniska kommunikationssystem i samhället, där användare kan sända och hämta elektroniska meddelanden. Dessa tjänster kan vara inrättade för de mest skiftande ändamål. Frågan om tillämpningsområdet för en lag om elektroniska förmedlingstjänster får därför stor praktisk betydelse.

Som framgått föreslår jag vissa undantag från DL:s regler om skydd för personlig integritet för sådana förmedlingstjänster som drivs för syften som skyddas av yttrandefrihetsgrundlagen. Med hänsyn till önskemålet att komma till rätta med brottsliga förfaranden och andra missbruk kan emellertid den särskilda lagens tillämpningsområde inte begränsas till sådana tjänster. Missbruk kan förekomma inom alla typer av tjänster, och om ett brådskande myndighetsingripande är befogat, bör den utredande myndigheten inte behöva inveckla sig i långdragna diskussioner med innehavaren om i vilket syfte han driver sin tjänst.

Jag föreslår därför, som redan framgått, att den särskilda lagen i princip skall gälla alla tjänster som avser förmedling av elektroniska meddelanden.

Lagen bör emellertid inte omfatta den som tillhandahåller endast nät eller andra förbindelser för överföring av elektroniska meddelanden. I telelagen finns bestämmelser för den som bedriver televerksamhet om bl.a. tystnadsplikt och utlämnande av uppgifter — en reglering som kommit till med sikte på dem som tillhandahåller nät. Den som endast tillhandahåller kommunikationslederna har vanligtvis inget inflytande över vilka tjänster som tillhandahålls och befordran brukar avse sådana datamängder att ett ansvar för vad som befordras inte är realistiskt.

Den särskilda lagen bör inte heller gälla för förmedling av elektroniska meddelanden inom en myndighet eller mellan myndigheter eller inom ett företag eller en koncern. Behovet av skyddsregler måste bedömas vara mindre inom ramen för sådana tjänster genom den tillsyn som organisationens ledning utövar. En viktig omständighet som väsentligt minskar risken för missbruk är härvid att användarna i sådana system inte torde ha möjlighet att sända meddelanden anonymt. Det kan dock invändas att också företagsinterna tjänster borde omfattas av det något större utrymme för ett fritt meningsutbyte som det föreslagna undantaget från DL:s regler om skydd för personlig integritet avses ge för vissa tjänster. Om det t.ex. i remissbehandlingen skulle visa sig att de fördelar som en tillämpning av den föreslagna lagen skulle kunna föra med sig anses väga tyngre än de olägenheter som tillämpningen av ordningsreglerna trots allt kan innebära, är det möjligt att ta bort det föreslagna undantaget. Det finns också möjlighet att införa en mellanform t.ex. så att interna tjänster som i övrigt uppfyller villkoren för att kunna utnyttja undantaget från DL, kan komma in under det nya systemet genom en anmälan till Datainspektionen.

Från den särskilda lagens tillämpningsområde bör också undantas sådana tjänster som omfattas av regleringen i TF eller YGL.[17]

Slutligen bör lagen endast delvis göras tillämplig på elektronisk post och andra elektroniska meddelanden som är avsedda bara för viss eller vissa mottagare. Bestämmelserna i 4 kap. BrB och 21 § DL till skydd mot olovlig åtkomst av elektroniska meddelanden bör i huvudsak gälla också inom ramen för tjänster för förmedling av elektroniska meddelanden; jfr dock avsnitt 11.4.5 och 12.3.3.

11.4 Regleringens huvudsakliga innehåll

11.4.1 Allmänt

För att gällande regelverk skall fungera i anknytning till elektroniska förmedlingstjänster behövs vissa anpassningar av såväl förmedlingstjänsterna som den straff- och processrättsliga regleringen. De komplikationer som har berörts i de inledande avsnitten utgörs bl.a. av svårigheter att kunna identifiera vilken förmedlingstjänst som är aktuell i ett enskilt fall, var den finns, vem som innehar den och vem som har gjort sig skyldig till ett missbruk av den. Om missbruk av elektroniska förmedlingstjänster skall kunna förhindras eller försvåras och det skall bli möjligt att, med rimliga insatser, komma till rätta med brottsliga eller i övrigt oacceptabla förfaranden behöver dessa hinder undanröjas. Sådana åtgärder förutsätter dock att den som innehar förmedlingstjänsten verkar för att rutinerna skall få en lämplig utformning. Som redan anförts bör därför en reglering införas som tar sikte på honom.

11.4.2 Vilka förmedlingstjänster avses

Som framgått av avsnitt 11.3.2 har digitaliseringen av kommunikationer och medier inneburit att gränserna mellan olika tillämpningar bryts igenom. Den enda bestående avgränsningen av de företeelser mitt uppdrag avser synes vara att de grundas på datorförmedlad överföring av meddelanden.

Naturligtvis bör den reglering jag föreslår innefatta sådana traditionella elektroniska anslagstavlor som användarna når genom att med modem ringa ett visst abonnentnummer. Det spelar härvid ingen roll om äldre teckenbaserade eller moderna användarvänliga programvaror med grafiskt gränssnitt används, och det är inte bara fora för gruppkommunikation som bör omfattas. Regleringen bör i princip gälla för samtliga de tjänster — och kombinationer av dessa — som har berörts

[17] Se avsnitt 11.3.2 angående vikten av att undvika särreglering för enskilda tillämpningar som — om man bortser från distributionssättet — är i det närmaste identiska med traditionella tjänster.

i avsnitt 10.1.3 samt anknytande och nya tillämpningar som växer fram. Detsamma bör gälla för tjänster som nås via Internet eller andra nät för datorkommunikation — t.ex. tjänster som tillhandahålls via World-Wide Web-servrar, Gopher-servrar eller listservrar — där en snabb utveckling av nya tjänster kan förutses. Avgörande bör vara om den som använder tjänsten kan ta del av information eller sända information till andra. En tillämpning som syftar till annat än att användarna skall kunna kommunicera, t.ex. när data översänds endast för matematiska beräkningar i en kraftfullare dator, utgör alltså inte en sådan tjänst som mitt förslag avser.

Ytterligare en begränsning ligger i att förslaget endast omfattar "tjänster" för elektronisk förmedling av meddelanden. En sådan tjänst föreligger inte vid manuell förmedling av meddelanden med tekniska hjälpmedel såsom faxar och datorer. Förmedlingen måste ske via tekniska och administrativa strukturer som datorer hanterar så att kommunikationen automatiseras eller annars underlättas. Beträffande elektroniska konferenser utgörs denna struktur vanligtvis av att meddelanden tekniskt styrs till en viss konferens, medan World-Wide Web ges struktur genom bl.a. hyperlänkarna.[18] Beträffande e-post sker viss strukturering genom adressering och ärendemeningar, varigenom meddelanden automatiskt kan förmedlas och sorteras av datorer, men också genom t.ex. nyckelord och länkar mellan meddelanden uppåt och nedåt i kedjor. Meddelanden som förmedlas via distributionslistor struktureras genom tillhörigheten till en viss lista. Tjänsterna för förmedling av elektroniska meddelanden gör det alltså möjligt att helt eller delvis automatisera kommunikation en-till-en, en-till-många och många-till-många.

Anledningen till att jag valt denna begränsning, i stället för uppräkningar av vissa tillämpningar, kan enkelt åskådliggöras av de olika möjligheter som finns att använda telefax. Faxmeddelanden överförs visserligen elektroniskt, men sådan vanlig faxkommunikation där användaren slår ett visst nummer så att linjen kopplas upp och faxet överförs bör naturligtvis inte omfattas av den särskilda regleringen. Efter uppkopplingen uppstår här, till skillnad från motsvarande uppkoppling till t.ex. en elektronisk anslagstavla, inte någon interaktiv kommunikation; det föreligger ingen "tjänst" som avser förmedling av meddelanden utöver de rena kopplingsfunktionerna i näten. Det är emellertid fullt möjligt att ersätta t.ex. distributionslistor för e-post med motsvarande rutiner för telefaxmeddelanden, och en sådan tjänst bör omfattas.[19]

[18] Se avsnitt 10.1.3 angående dessa begrepp.

[19] Rutinerna kan utformas så att inkommande faxmeddelanden automatiskt sänds till alla adressater som tillhör en viss grupp. Härvid saknar teknikvalet vid transporten via nät (analogt eller digitalt) betydelse. Det avgörande är att informationen behandlas digitalt såväl vid inläsning hos avsändaren som vid behandling hos mottagaren.

Vissa andra verksamheter bör som framgått av avsnitt 11.3.5 helt undantas. Detta gäller tillhandahållande endast av nät eller andra förbindelser för överföring av elektroniska meddelanden, förmedling av meddelanden inom en myndighet eller mellan myndigheter eller inom ett företag eller en koncern samt tjänster som omfattas av regleringen i TF eller YGL (1 § andra stycket förslaget till lag om elektroniska förmedlingstjänster). Undantaget omfattar alltså t.ex. program i ljudradio eller television.

Jag återkommer i avsnitt 11.6 till frågan om en avgränsning mot telelagens tillämpningsområde.

11.4.3 Registrering av förmedlingstjänster eller andra åtgärder för att peka ut en ansvarig?

Svårigheterna att identifiera elektroniska förmedlingstjänster skulle, efter förebild av bestämmelserna i DL om anmälan och licens, kunna begränsas genom ett särskilt registreringsförfarande för förmedlingstjänster. Erfarenheterna av systemet med licens har emellertid föranlett en strävan att frångå sådana rutiner.

Man kan räkna med att ett krav på registrering av elektroniska förmedlingstjänster skulle efterlevas av dem som driver en öppen och seriös verksamhet och medföra ett inte obetydligt administrativt arbete för dem och — framför allt — för den myndighet som skulle ha hand om registreringen. Däremot är det inte sannolikt att ett sådant krav i någon större utsträckning skulle följas av innehavarna av sådana förmedlingstjänster där mer flagranta missbruk förekommer. Ett registreringskrav skulle alltså knappast undanröja svårigheterna att identifiera sådana tjänster. Inte heller ser jag det som någon fördel att innehavaren av en sådan förmedlingstjänst — när han väl hade identifierats — skulle kunna straffas för brott mot registreringsplikten. Om det har förekommit brott mot de regler för driften av en elektronisk förmedlingstjänst som jag föreslår i det följande, är det tillräckligt att straff kan utdömas för detta. Om å andra sidan förmedlingstjänsten har skötts på ett oklanderligt sätt, skulle det saknas rättspolitisk grund för ett straff på grund av utebliven registrering.

Jag föreslår i stället andra åtgärder för att det skall kunna klarläggas vilken förmedlingstjänst som är aktuell och vem som ansvarar för den. En åtgärd jag har övervägt är att föreskriva en skyldighet för den som äger eller annars förfogar över det informationssystem där en förmedlingstjänst drivs (systemägaren) att utse en ansvarig för tjänsten (systemansvarig), samt att uppställa vissa krav på den systemansvariges

personliga kvalifikationer m.m.[20] Ett sådant regelverk för ägare av informationssystem respektive denne särskilt utpekade ansvarige torde emellertid bli alltför komplicerat och det kan bli svårt att, inom ramen för nära nog gränslösa kommunikationsmöjligheter, peka ut ett visst informationssystem. Det skulle vidare bli resurskrävande för den som innehar omfattande informationssystem.

I stället föreslår jag vissa åligganden för den som tillhandahåller en elektronisk förmedlingstjänst — bl.a. skyldighet att informera om vem som tillhandahåller tjänsten, att ha uppsikt över den och att förhindra fortsatt spridning av vissa meddelanden. Det nu vanliga förfaringssättet att den som driver en förmedlingstjänst anger endast täcknamn (s.k. "handles") bör alltså inte tillåtas. Var och en bör alltså omgående kunna få besked om vem som tillhandahåller tjänsten och denna underrättelseskyldighet bör straffsanktioneras (4 och 6 §§ förslaget till lag om elektroniska förmedlingstjänster).

Jag föreslår att underrättelseskyldigheten lagtekniskt utformas så att den som vill använda tjänsten skall få en sådan underrättelse så snart det kan ske. Underrättelsen kan vanligtvis antas komma att lämnas i ett meddelande som möter den som anropar tjänsten, bl.a. för att undvika administrativt arbete för den ansvarige.

Genom att en sådan informationsskyldighet införs bör det bli lätt för myndigheter och enskilda att få veta vem de skall vända sig till.[21]

11.4.4 Vem bör regleringen riktas mot

Jag föreslår alltså att vissa krav ställs på *den som tillhandahåller* en tjänst som avser förmedling av elektroniska meddelanden. Frågan är då vem denne är.[22] Inte heller här är det möjligt att göra någon fullständig genomgång av olika förmedlingstjänster och kategorier av personer som är knutna till sådana tjänster.

När tjänsten inte tillhandahålls av en juridisk person eller en myndighet bör frågan om vem den föreslagna regleringen riktas mot vara enkel att besvara. Det finns helt enkelt en person som uppenbarligen är den som leder verksamheten, och denne torde i de allra flesta fallen pekas ut i den information till användarna som krävs enligt förslaget till lag om elektroniska förmedlingstjänster. Beträffande

[20] Det skulle kunna förbjudas att t.ex. den som är bosatt utom Sverige eller är underårig eller i konkurs eller har förvaltare enligt 11 kap. 7 § föräldrabalken utses som systemansvarig.

[21] Jag föreslår visserligen inte något centralt register över elektroniska förmedlingstjänster, men mina förslag bör göra det möjligt för polisen att få underrättelse från teleoperatörer om vem som innehar en viss teleadress, och straffprocessuella åtgärder kan komma i fråga.

[22] Jfr legaldefinitionen i 1 § DL av registeransvarig. I praxis har vissa svårigheter uppstått att bestämma på vem detta ansvar vilar; se vidare Datalagsutredningens betänkande En ny datalag (SOU 1993:10), 12 kap.

tjänster av mindre omfattning kan dessutom fysiska och tekniska realiteter ge vägledning. Den dator som används för att tillhandahålla tjänsten kanske finns i en lägenhet som innehas av en viss person. Om det i stället är ett större informationssystem som används kan det vara så att endast *en* person, till följd av behörighetskontrollsystem, har befogenheter att t.ex. radera eller annars vidta ingripande åtgärder med avseende på tjänsten. När många är engagerade i den övergripande hanteringen av tjänsten kan frågan bli mera komplicerad.[23]

Eftersom jag har föreslagit en skyldighet att vid straffansvar underrätta om vem som tillhandahåller en förmedlingstjänst, torde frågan ställas på sin spets från straffrättsliga utgångspunkter. Det är inget nytt att ett visst subjekt pekas ut som ansvarig; se t.ex. 2 kap. 29 § ordningslagen (1993:1617), där det föreskrivs om ansvar för den som i egenskap av "anordnare" bryter mot bl.a. krav på tillstånd eller anmälan, samt 164 och 165 §§ vägtrafikkungörelsen (1972:603), där "ägare" eller "innehavare" av viss egendom bär straffansvaret för vissa fall. Frågan om vem som tillhandahåller tjänsten får härvid avgöras utifrån en samlad bedömning av vem som har det bestämmande inflytandet över förmedlingstjänsten, och det får naturligtvis bortses från felaktiga uppgifter som lämnas till användarna om vem som tillhandahåller tjänsten. Därvid kan inte uteslutas att det i några fall inte går att finna någon ansvarig. Exempelvis kan en person som inte existerar eller som inte har något att göra med förmedlingstjänsten ha pekats ut som tillhandahållare. För sådana fall ger emellertid den reglering jag föreslår grund för att ingripa mot verksamheten.

När en juridisk person eller en myndighet tillhandahåller förmedlingstjänsten aktualiseras frågan om vilken eller vilka fysiska personer som i förevarande sammanhang skall anses företräda den juridiska personen eller myndigheten; juridiska personer kan inte föröva brott. Här får på vanligt sätt tillämpas de allmänna principer som har vuxit fram i praxis angående placeringen av ansvaret vid lagöverträdelser. Detta ansvar kan alltså under vissa förutsättningar delegeras, till skillnad från registeransvar enligt DL.[24]

En inte helt ovanlig situation är att den som svarar för t.ex. en elektronisk konferens upphör med sin verksamhet och att någon annan tar över. Här innebär den föreslagna särskilda lagen en skyldighet att vid straffansvar underrätta om att någon annan fortsättningsvis tillhandahåller tjänsten, och det bör ligga i den avgångnes intresse att inte längre pekas ut.

[23] Det är i och för sig möjligt att ge alla användare fullständig teknisk behörighet eller att använda informationssystemen så att det blir oklart på vilken fysisk plats de tekniska hjälpmedlen för en viss tjänst finns.

[24] Se bl.a. Thornstedt, Vissa specialstraffrättsliga problem, Ds Ju 1975:23 och Jareborg, Straffrättens gärningslära, 1995, s. 75 f., jfr SOU 1993:10 s. 320 och 377.

Det som nu har sagts hindrar inte att den som tillhandahåller tjänsten uppdrar åt någon annan att på hans vägnar handha skötseln av tjänsten, och jag återkommer till frågan om ansvar för denne (se vidare avsnitt 11.4.6)

11.4.5 E-post och slutna grupper

Som jag redan anfört i avsnitt 11.3.5 bör den särskilda lagen endast delvis göras tillämplig på e-post och andra meddelanden som är avsedda bara för viss eller vissa mottagare; jfr sådan kommunikation som sker med vanlig post. Som närmare utvecklas i avsnitt 12.3.3 föreskrivs straffansvar för den som olovligen bereder sig tillgång till elektroniska meddelanden (se 4 kap. BrB och 21 § DL). Frågan om gränsen för straffskyddets omfattning i IT-miljö har behandlats av Datastraffrättsutredningen,[25] där det framgår att saken är av sådan grundläggande och principiell karaktär att den inte kan genomlysas i detta begränsade sammanhang. Skyddet mot informationsintrång utesluter emellertid inte att de föreslagna bestämmelserna om undantag från DL och om information till användarna med anknytande bestämmelser om straff och förverkande (2, 4, 6 och 7 §§ förslaget till lag om elektroniska förmedlingstjänster) tillämpas även beträffande tjänster för e-post. Som berörs i det följande föreslår jag vidare en bestämmelse om att den som tillhandahåller tjänsten skall ha viss uppsikt över denna (3 §), en regel som kan tillämpas också på en tjänst för förmedling av e-post så länge den som tillhandahåller tjänsten inte olovligen gör intrång i sådana meddelanden.

Annorlunda förhåller det sig med den sanktionerade skyldigheten att förhindra fortsatt spridning (förslaget i 5 §). På motsvarande sätt som posten inte svarar för innehållet i de brev som befordras bör inte heller den som tillhandahåller en tjänst för e-post[26] åläggas nya skyldigheter med avseende på meddelanden till viss eller vissa adressater. Detta framgår av att den föreslagna bestämmelsen om förhindrande av spridning inte skall gälla meddelanden som är avsedda bara för viss eller vissa individuella mottagare (5 § andra stycket).

Det nu sagda innebär naturligtvis inte att all kommunikation som sker under beteckningen e-post automatiskt skall falla utanför de bestämmelser jag föreslår om förhindrande av vidare spridning (5 § första stycket och straffbestämmelsen i 6 §). Om någon användare t.ex. med hjälp av en distributionslista gör ett meddelande tillgängligt för en mängd användare, får situationen naturligtvis behandlas på samma sätt

[25] SOU 1992:110 s. 175 f.

[26] Här avses naturligtvis inte meddelanden som via förmedlingstjänsten blir tillgängliga för andra än adressaten.

som när meddelandet görs tillgängligt för alla användare av t.ex. en elektronisk anslagstavla. Här vore det visserligen praktiskt med en knivskarp avgränsning utifrån t.ex. vad som görs tillgängligt för fler än tio användare. En sådan reglering skulle emellertid lätt kunna kringgås, t.ex. genom indelningar i undergrupper av nio användare.

Vanligtvis torde det redan av tjänsternas utformning tveklöst framgå huruvida det är fråga om "privat" post eller kommunikation med en grupp. I tveksamma fall bör ledning kunna hämtas från analogier med traditionella försändelser, och det får utifrån ändamålet med kommunikationen avgöras om den skall anses vara avsedd bara för viss eller vissa användare eller för en grupp användare.

När fråga är om meddelanden som är avsedda att göras tillgängliga för en större krets av användare, är det ändå vanligt att kretsen begränsas till vissa användare, och att endast dessa ges tillgång till t.ex. den elektronisk konferens där meddelandena finns. Enligt min mening bör dock den som tillhandahåller den förmedlingstjänst där en sådan *sluten konferens* förekommer alltid ha rätt att ta del av meddelandena, oberoende av om han tillhör den slutna gruppen. Motsatt synsätt skulle göra det alltför lätt att kringgå den föreslagna regleringen. I denna del ger alltså den föreslagna särskilda lagen en laga befogenhet för den som är ansvarig för förmedlingstjänsten att ta del av all gruppkommunikation som förekommer där; jfr avsnitt 12.3.3.

11.4.6 Ansvarets närmare innebörd

När det så gäller den närmare innebörden av ansvaret, bör en utgångspunkt vara att den som tillhandahåller tjänsten inte bör få gå med på eller passivt se på när användare missbrukar tjänsten. Teknikens flexibilitet och tillgängligheten via nät medför särskilda risker för sådant missbruk. Jag föreslår därför en föreskrift om att den som tillhandahåller tjänsten skall vara skyldig att ha sådan uppsikt över tjänsten som är nödvändig med hänsyn till omfattningen och inriktningen av verksamheten (3 § förslaget till lag om elektroniska förmedlingstjänster). Genom den föreslagna regleringen ges den som tillhandahåller tjänsten en sådan garantställning att ansvar kan komma i fråga för medverkan till brott genom underlåtenhet att ingripa mot missbruk av tjänsten (se vidare avsnitt 12.3.1).

Som framgått bör också en skyldighet föreligga för den som tillhandahåller tjänsten att aktivt se till att elektroniska meddelanden med straffbart eller annars oacceptabelt innehåll inte får fortsatt spridning (5 § första stycket första meningen förslaget till lag om elektroniska förmedlingstjänster). De meddelanden mot vilka ingripande bör ske kan delas in i tre kategorier.

En kategori utgörs av meddelanden med sådant innehåll att användaren genom att sända in meddelandet gör sig skyldig till brott. Det kan

vara fråga om t.ex. främlingsfientlig propaganda. En annan kategori utgörs av upphovsrättsligt förbjuden programkopiering som inte är straffsanktionerad. En tredje kategori av meddelanden har sådant innehåll att de är ägnade att användas vid brott, såsom hemliga koder för tillträde till informationssystem, kontokortsnummer och uppgifter för att begå telebedrägerier.

Om den som tillhandahåller tjänsten själv har den faktiska uppsikten över tjänsten, är det naturligtvis också han själv som skall stoppa fortsatt spridning av meddelanden av detta slag. Om han har uppdragit åt någon annan att hålla den löpande uppsikten över tjänsten, bör denne på samma sätt vara skyldig att ingripa mot den angivna kategorin av meddelanden (5 § första stycket andra meningen förslaget till lag om elektroniska förmedlingstjänster).[27]

Om regler av det nu skisserade slaget infördes utan modifikationer, skulle man från praktiskt håll med fog kunna invända att reglerna skulle vara omöjliga att följa. Informationsflödet är i de flesta fall alldeles för stort för att den som tillhandahåller tjänsten skall kunna systematiskt granska de meddelanden som förmedlas. Med hänsyn till att många tjänster tillhandahålls av amatörer — ofta ungdomar — är det inte heller realistiskt att begära att den som tillhandahåller tjänsten skall kunna göra några mer subtila bedömningar av vilka meddelanden som kan innefatta brott osv. Jag föreslår därför två begränsningar av skyldigheten att hindra fortsatt spridning av oacceptabla meddelanden. Dessa begränsningar — som också sammanhänger med att skyldigheten att aktivt hindra fortsatt spridning av oacceptabla meddelanden enligt min mening bör vara straffsanktionerad (se avsnitt 11.4.9) — medför att inte ens den som hanterar mycket stora informationsmängder ställs inför några orimliga krav.

För det första bör skyldigheten att vara aktiv för att hindra fortsatt spridning av oacceptabla meddelanden i praktiken inte inträda förrän den ansvarige (eller den som för hans räkning har uppsikt över tjänsten) får kännedom om vad som pågår. Det betyder visserligen inte att den ansvarige kan förhålla sig helt passiv, eftersom han enligt 3 § i den föreslagna lagen har en allmän plikt att hålla uppsikt över tjänsten, men den mer konkreta handlingsplikten enligt 5 § bör inte inträda förrän han har fått klart för sig att det förekommer brottsliga eller annars oacceptabla meddelanden. Kännedom om detta kan han få t.ex. genom att han själv ser ett meddelande som inte bör spridas vidare eller genom att en användare på något sätt gör honom uppmärksam på att det förekommer olämpliga meddelanden i någon viss del av hans tjänst. Jag har

[27]Här syftas inte på sådana situationer där det rättsliga ansvaret för att en viss föreskrift följs kan delegeras till t.ex. en avdelningschef i ett större företag; se Thornstedt, Ds Ju 1975:23 s. 93 f. och 128 f. När sådan delegation har skett är det den till vilken delegation har skett som "tillhandahåller tjänsten".

övervägt att direkt i 5 § ange att skyldigheten inträder endast när den ansvarige har kännedom om förhållandet. Detta följer emellertid, som jag återkommer till i avsnitt 11.4.9, redan av att den anknytande bestämmelsen om straffansvar gäller endast om uppsåt föreligger.

För det andra bör skyldigheten att hindra fortsatt spridning bara gälla om det är *uppenbart* att en användare genom att sända in ett elektroniskt meddelande har gjort sig skyldig till brott eller intrång i upphovsrätt eller att innehållet i ett meddelande är ägnat att användas vid brott. Det är alltså bara när det för en genomsnittligt eftertänksam person skulle vara tydligt t.ex. att innehållet i ett meddelande är ägnat att användas vid brott som något ingripande bör krävas.

Skyldigheten att förhindra fortsatt spridning av sådana meddelanden innebär inte att materialet skall utplånas hos den som är ansvarig för tjänsten. Data som behövs t.ex. för att utreda och bevisa brott bör inte få förstöras (jfr 14 kap. 4 § och 15 kap. 8 § BrB).

I den yttrandefrihetsrättsliga regleringen föreskrivs att framställningar skall bevaras under viss tid efter att de har offentliggjorts. Bekämpningen av missbruk av elektroniska förmedlingstjänster skulle effektiviseras på motsvarande sätt om krav ställdes på bevaring av elektroniska meddelanden och uppgifter om användare under viss tid. Jag föreslår emellertid inte någon bestämmelse om bevaring, dels med hänsyn till de stora datamängder det skulle kunna bli fråga om, dels på grund av de administrativa komplikationer det skulle innebära. För att en sådan reglering skall bli meningsfull krävs nämligen att den som tillhandahåller tjänsten också upprättar och bevarar systemdokumentation och håller tekniska hjälpmedel tillgängliga för att läsa data även om han har bytt datorer och programvaror. Upptagningar vid myndigheters elektroniska anslagstavlor som blir allmänna handlingar måste dock ofta bevaras; se avsnitt 6.4.

11.4.7 Registrering och uteslutning av användare?

När användare tillåts att sända in meddelanden till en elektronisk förmedlingstjänst så att meddelandena blir omedelbart tillgängliga för övriga användare framträder särskilda risker för missbruk. Det har nämligen visat sig svårt, ofta omöjligt, att klarlägga vem som ligger bakom brottsliga förfaranden. Det vore därför värdefullt med en föreskrift om att den som tillhandahåller förmedlingstjänsten fick tillåta att meddelanden görs direkt tillgängliga endast om han registrerade och verifierade användarnas identitet på ett sådant sätt att användare som missbrukar förmedlingstjänsten kunde identifieras. Därmed skulle de brottsutredande organen få ökade möjligheter att rikta sina åtgärder mot den som är upphovet till ett missbruk av en förmedlingstjänst. En sådan regel skulle inte innebära att namnet på den som ligger bakom viss

information måste vara utsatt när meddelandet sprids, utan det vore tillräckligt att förmedlaren bevarade uppgifterna om ursprung.

I praktiken är emellertid en sådan reglering för närvarande inte möjlig. Stora delar av de diskussionsgrupper som kan nås via t.ex. Internet är åtkomliga helt utan kontroller av vem det är som använder tjänsten och detsamma gäller huvuddelen av de elektroniska anslagstavlorna i Sverige. Visserligen finns det, som framgår av del I och bilaga 2, säkra tekniska rutiner för att verifiera användare och utställare av handlingar. Sådana rutiner är emellertid inte allmänt spridda ännu och de torde kräva en så omfattande administration att användningen av elektroniska förmedlingstjänster kunde komma att kvävas. Jag föreslår därför inte någon sådan reglering.

För förmedlingstjänster där den allmänt tillgängliga informationen är modererad, dvs. där en viss person har bestämt vilka meddelanden som skall bli allmänt tillgängliga, torde detta inte heller behövas. Det är tillräckligt att uppgifter bevaras om vem som tillhandahåller tjänsten. I den mån brottsligt material förekommer bör denne i tillräcklig omfattning kunna ställas till ansvar för att ha gjort uppgifterna tillgängliga. Inget hindrar dock att den som uppgifterna härrör från ställs till ansvar, om han kan identifieras.

I de fall där insända meddelanden blir direkt tillgängliga för övriga användare kan en användare missbruka förmedlingstjänsten genom att t.ex. gång på gång sända in meddelanden med brottsligt innehåll. Även om den som tillhandahåller förmedlingstjänsten så fort det kan ske hindrar fortsatt spridning, är risken stor att meddelandena når en större krets, t.ex. via en distributionslista. Det kunde därvid ifrågasättas om inte den som tillhandahåller tjänsten borde vara skyldig att utesluta användaren.

Enligt min mening är det dock inte nödvändigt att införa bestämmelser om uteslutning från elektroniska förmedlingstjänster. Det får anses tillräckligt med den självsanering som torde bli följden av skyldigheten för den som är ansvarig för tjänsten att förhindra fortsatt spridning av vissa meddelanden.

11.4.8 En skyldighet att informera

Enligt 10 § första stycket DL skall den registeransvarige på begäran av enskild så snart det kan ske underrätta denne antingen om innehållet i personuppgift som ingår i personregistret och innefattar upplysning om honom eller om att sådan uppgift inte förekommer i registret. Frågan är om liknande bestämmelser bör införas för elektroniska förmedlingstjänster.

Den som själv är användare och har oinskränkt åtkomst till förmedlingstjänsten bör naturligtvis inte ha rätt till sådan underrättelse eftersom han kan ta del av uppgifterna elektroniskt. Frågan är då om

det i övrigt bör införas någon skyldighet för den som tillhandahåller tjänsten att på begäran underrätta den som är registrerad.

En sådan skyldighet skulle föra med sig vissa komplikationer. Bestämmelsen i 10 § DL har tillkommit för att tillgodose behovet av insyn i egentliga register. Sådana register har emellertid en struktur som gör det möjligt att söka fram alla uppgifter som är registrerade om en viss person. Elektroniska meddelanden — inklusive bilder och datorprogram — vid elektroniska förmedlingstjänster saknar däremot den struktur som krävs för att uppgifter om en viss person skall kunna sammanställas automatiskt. Visserligen finns funktioner för fritextsökning, men det är snarare regel än undantag att personer beskrivs med täcknamn eller annars så att uppgifterna inte kan sökas automatiskt. Vidare kan flera personer bära samma namn, och förekomsten av ett visst namn i en viss del av den löpande texten behöver inte innebära att det finns upplysningar om denne just i det textavsnittet. Bildfiler och datorprogram kan inte heller, utan speciella åtgärder, genomsökas efter personuppgifter.

Ett krav på utdrag beträffande löpande text vid elektroniska förmedlingstjänster torde därför leda till att avancerade program införs för att söka och sammanställa personuppgifter, samtidigt som en omfattande manuell hantering krävs för att tillskapa korrekta utdrag. Ett krav på utdrag beträffande löpande text skulle på detta sätt alltså föra med sig ökade risker för otillbörligt integritetsintrång. Detta gäller särskilt som användarna, vilka enligt det ovan sagda skulle ha att själva ta fram vad som har registrerats om dem, rimligen också bör få tillgång till de sökmöjligheter som införs.[28]

En avvägning mellan den nytta resp. de risker för den enskilde som sådana rutiner skulle föra med sig, leder enligt min mening till att det inte bör föreskrivas någon underrättelseskyldighet med avseende på löpande text beträffande vilken den särskilda lagen — inte DL — skall tillämpas.

Detsamma bör gälla för egentliga register över elektroniska meddelanden och användare vid elektroniska förmedlingstjänster. Dessa uppgifter har tillförts under medverkan av den enskilde, som vanligtvis kan ta del av dem elektroniskt.

Däremot finns det skäl att ålägga den som tillhandahåller en elektronisk förmedlingstjänst att ge viss annan information. Eftersom sådana tjänster är en relativt ny företeelse är det sannolikt att många

[28] Förutsättningarna påminner om vad som gäller för elektroniska akter enligt skatteregisterlagen (1980:343). Där har undantag föreskrivits från 10 § DL; se 18 § skatteregisterlagen, 10 a § utsökningsregisterlagen och mitt förslag till en ny 10 a § DL. Handlingarna i de elektroniska akterna är till stora delar lagrade som bilder och kan således inte genomsökas automatiskt. Vidare har begränsningar införts när det gäller terminalåtkomst till akterna. Sökning av om uppgifter om en viss person finns i andra akter än dem som rör honom får inte ske.

som ansluter sig till en förmedlingstjänst inte fullt ut förstår konsekvenserna av att sända och motta meddelanden. Den som tillhandahåller tjänsten bör därför vara skyldig att informera de användare som ansluter sig till tjänsten om vissa särskilt betydelsefulla följder av det elektroniska informationsutbytet.

Jag föreslår därför en skyldighet för den som tillhandahåller tjänsten att underrätta dem som vill ansluta sig om i vilken utsträckning inkomna meddelanden blir tillgängliga för andra användare och om att användaren är ansvarig för innehållet i de elektroniska meddelanden han sänder in (4 § första stycket förslaget till lag om elektroniska förmedlingstjänster). I myndigheters elektroniska förmedlingstjänster skall den som tillhandahåller tjänsten underrätta användarna också om att de meddelanden som förmedlas kan bli allmänna handlingar (4 § andra stycket); i avsnitt 11.4.3 har jag redan föreslagit ett krav på underrättelse om vem som tillhandahåller förmedlingstjänsten.

11.4.9 Straffansvar, förverkande och skadestånd

Som framgått föreslår jag inget krav på licens eller tillstånd för att inrätta och driva en elektronisk förmedlingstjänst. Samtidigt ges den som tillhandahåller tjänsten vissa skyldigheter som är av grundläggande betydelse för möjligheterna att tillgodose de olika skyddsintressen som aktualiseras vid sådan kommunikation. Jag föreslår en bestämmelse i den särskilda lagen (6 §) om straffansvar för den som bryter mot lagens regler om information till användarna (4 §) och förhindrande av fortsatt spridning av brottsliga eller annars oacceptabla meddelanden (5 §).

Ansvar för brott mot 4 § bör inträda både för uppsåtliga gärningar och för gärningar som begås av oaktsamhet. Beträffande brott mot 5 § — som torde vara det praktiska fallet — bör däremot endast uppsåtliga gärningar föranleda ansvar. En regel om ansvar redan vid oaktsamhet skulle skapa alltför stor osäkerhet om ansvarets omfattning när stora informationsmängder hanteras. Ansvaret bör vila på den som har den faktiska möjligheten att förhindra fortsatt spridning. Om den som tillhandahåller tjänsten har uppdragit åt någon annan att hålla uppsikt över tjänsten, bör alltså denne kunna straffas om han uppsåtligen låter bli att förhindra fortsatt spridning av oacceptabla meddelanden. Beroende på omständigheterna kan naturligtvis både den som tillhandahåller tjänsten och den som på hans uppdrag har uppsikt över tjänsten bli ansvariga för att samma meddelande har fått fortsatt spridning.

För att undvika lagföring av bagatellartade förseelser föreslår jag att det i ringa fall inte skall dömas till ansvar.

I syfte att undvika de tolknings- och tillämpningssvårigheter som frågor om konkurrens med bestämmelserna i brottsbalken aktualiserar, föreslår jag vidare att ansvar enligt den särskilda lagen inte skall inträda om straff kan ådömas enligt brottsbalken (6 § andra stycket). Detta kan

bli aktuellt t.ex. om den som tillhandahåller tjänsten tillåter spridning av främlingsfientliga meddelanden under sådana omständigheter att han ådrar sig ansvar för medverkan till användarens brott (hets mot folkgrupp).

Jag föreslår också en anpassning av vissa straffbestämmelser i 16 kap. BrB till de särskilda förhållanden som råder vid kommunikation via elektroniska förmedlingstjänster. Jag återkommer till dessa frågor i avsnitt 12.2.1.

Vid sidan av straff bör det vara möjligt att förklara datorer och andra hjälpmedel förverkade. Ett förverkande kan, när den som tillhandahåller en förmedlingstjänst inte bryr sig om att följa de föreslagna reglerna, vara ett kännbart komplement till straff eller annan påföljd, samtidigt som risken för fortsatt brottslighet därigenom kan minskas.

Vissa bestämmelser i 36 kap. brottsbalken om förverkande är tillämpliga också vid brott mot en straffbestämmelse i specialstraffrätten. Detta gäller bl.a. 3 § enligt vilken förverkande får beslutas bl.a. i fråga om föremål som på grund av sin särskilda beskaffenhet och omständigheterna i övrigt kan befaras komma till brottslig användning. Bestämmelsens räckvidd är emellertid begränsad, bl.a. genom att föremålet som sagt skall vara av sådan särskild beskaffenhet att det kan befaras komma till brottslig användning; jfr HD:s dom den 22 februari 1996, DB 27.

I 36 kap. 2 § brottsbalken föreskrivs vidare att egendom som använts som hjälpmedel vid brott må förklaras förverkad, om det är påkallat till förebyggande av brott eller eljest särskilda skäl föreligger. Bestämmelsen, som ansluter till den här aktuella situationen, är emellertid tillämplig endast vid brott enligt brottsbalken.

Jag föreslår därför att det föreskrivs att datorer och andra hjälpmedel, såsom datorprogram, som har använts vid brott enligt den föreslagna lagen skall kunna förklaras förverkade, om åtgärden behövs för att förebygga brott eller det annars finns särskilda skäl (7 § förslaget till lag om elektroniska förmedlingstjänster). Det kan ofta antas att risk för fortsatt brottslighet föreligger om en förmedlingstjänst i större omfattning har innehållit t.ex. hemliga tillträdeskoder, kontokortsnummer, s.k. piratkopior av datorprogram, främlingsfientligt material, etc.[29]

Enligt 23 § DL gäller ett strängt skadeståndsansvar för den registeransvarige. Om en registrerad person tillfogas skada genom att personregistret innehåller oriktiga eller missvisande uppgifter om honom, är den registeransvarige skadeståndsskyldig oberoende av vållande, och vid skadebedömningen skall hänsyn tas även till lidande och andra omständigheter av annan än rent ekonomisk betydelse.

[29] Jfr uttrycket "tekniskt hjälpmedel", som innefattar också datorprogram och andra data (prop. 1994/95:227 s. 28 f.). Ang. de särskilda komplikationer som framträder i IT-miljön, se SOU 1992:110 s. 395 f.

Det är uppenbart att man inte bör införa ett sådant ansvar för den som tillhandahåller en elektronisk förmedlingstjänst; en sådan regel skulle helt omöjliggöra verksamheten. Det är också klart att den som tillhandahåller tjänsten även utan någon regel i den särskilda lagen kan bli skadeståndsskyldig på samma sätt som en användare om han sprider ett meddelande med ett skadeståndsgrundande innehåll. Frågan är då om det bör införas en särskild regel som — utan att gå lika långt som 23 § DL — gör det lättare för en skadelidande att få ersättning av den som tillhandahåller tjänsten.

För att den skadelidande skall kunna få skadestånd enligt allmänna skadeståndsrättsliga regler, av den som tillhandahåller förmedlingstjänsten, med anledning av att ett meddelande som innefattar t.ex. förtal eller upphovsrättsligt förbjuden programkopiering har spritts, torde åtminstone krävas att den ansvarige har känt till meddelandets innehåll och karaktär innan meddelandet spreds, något som det ofta är mycket svårt för den skadelidande att bevisa. Som framgått är det samtidigt inte rimligt att ålägga den som tillhandahåller tjänsten ett allmänt ansvar för innehållet i de meddelanden som sprids via förmedlingstjänsten; det skulle alltför mycket strida mot önskemålet om ett i princip fritt informationsflöde.

Enligt min mening får de ökade möjligheterna till ersättning för ren förmögenhetsskada som blir följden av den straffbestämmelse jag föreslår i den särskilda lagen anses vara en rimlig avvägning mellan motstående intressen av ett fritt informationsflöde respektive ersättning för skada.

11.5 Tillsyn

Det finns ett behov av statlig tillsyn på området för elektronisk kommunikation. Personregister vid förmedlingstjänster som inte avses med det undantag från DL som jag föreslagit innefattas i Datainspektionens tillsynsverksamhet (15 § DL). På motsvarande sätt kan tillsyn aktualiseras enligt telelagen genom Post- och telestyrelsen (31 § telelagen), i den mån telelagen är tillämplig på verksamheter vid elektroniska förmedlingstjänster (se vidare nästa avsnitt). Detta illustrerar väl hur mitt uppdrag rör olikartade företeelser som bryter igenom traditionella gränser.

Så som mitt förslag till en särskild lag om elektroniska förmedlingstjänster slutligen har utformats aktualiseras i huvudsak endast sådana ingripanden och åtgärder som hör till de brottsutredande myndigheternas verksamhetsområde. Jag föreslår därför inte någon utvidgning av Datainspektionens eller Post- och telestyrelsens verksamhet för tillsyn.

11.6 Konkurrerande regler i datalagen, telelagen och den särskilda lagen

Skyddsreglerna i den särskilda lagen behövs också utanför det yttrandefrihetsrättsliga området, samtidigt som behovet av persondataskydd gör sig gällande. Därför kan reglerna i DL och den särskilda lagen bli aktuella samtidigt. Härvid aktualiseras främst reglerna om vem som är registeransvarig respektive tillhandahåller förmedlingstjänsten. Här vore det visserligen naturligt att, med utgångspunkt från den särskilda lagens karaktär av specialbestämmelser för elektroniska förmedlingstjänster, anse att den som tillhandahåller förmedlingstjänsten också bör vara registeransvarig enligt DL för sådana egentliga register som undantagsvis kan förekomma vid tjänsten och för vilka DL är tillämplig. En sådan bedömning skulle emellertid öppna vägen för kringgående av de nuvarande reglerna i DL, som innebär bl.a. att registeransvaret inte kan delegeras.

I telelagen (1993:597) finns bestämmelser om bl.a. förbud mot avlyssning, tystnadsplikt och skyldighet att lämna uppgifter till brottsutredande myndigheter (24 - 27 §§), bestämmelser som i någon mån kan konkurrera med regleringen i den särskilda lagen.

Bestämmelserna i telelagen är tillämpliga i "televerksamhet", vilket definieras som förmedling av telemeddelanden via telenät eller tillhandahållande av förbindelser för sådan verksamhet. Telenät definieras som anläggning för förmedling av telemeddelanden. Enligt telelagens ordalydelse innefattas alltså även sådana förmedlingstjänster som jag föreslår skall regleras särskilt.

Telelagen har dock tillkommit från andra utgångspunkter än mitt förslag, och frågan om i vilken omfattning telelagen bör tillämpas på elektroniska förmedlingstjänster har, såvitt framgår av lagmotiven, inte övervägts i det lagstiftningsärendet. Härvid aktualiseras grundläggande och principiella straffrättsliga och straffprocessuella frågor. Bör den som tillhandahåller en förmedlingstjänst ha rätt att för vissa syften ta del av elektroniska meddelanden som i och för sig skyddas av straffbestämmelser angående intrång i information? Vilka skyldigheter bör den som tillhandahåller tjänsten ha att aktivt samverka med brottsutredande myndigheter? Sådana principiella frågor bör, som jag återkommer till avsnitt 12.4.1, övervägas i ett större sammanhang.[30]

[30] De har tagits upp av Datastraffrättsutredningen och i en Europarådsrekommendation, No. R (95) 13, angående straffprocessuella frågor på IT-området. I rekommendationen art. 11 och 12 behandlas "operators of public and private networks that offer telecommunications services to the public" respektive "service providers who offer telecommunications services to the public", där mer långtgående krav ställs på den första kategorin. Uttrycket "service provider" avses enligt motiven till rekommendationen innefatta den som tillhandahåller t.ex. en tjänst för elektronisk post men inte den som tillhandahåller en databas via nät.

Fråga gäller alltså inte vilket tillämpningsområde den särskilda lagen om elektroniska förmedlingstjänster bör ha utan vilka avgränsningar som bör göras med utgångspunkt från de intressen som motiverar den aktuella regleringen i telelagen. För närvarande pågår också inom Kommunikationsdepartementet en översyn av telelagen. En departementspromemoria beräknas avlämnas under juni detta år och jag har inhämtat att man avser att ta upp också frågan om telelagens tillämpningsområde.

11.7 Nationella begränsningar

De elektroniska förmedlingstjänsternas gränsöverskridande karaktär aktualiserar frågan om den föreslagna särskilda lagen och bestämmelserna i vissa andra författningar är tillämpliga endast på förhållanden i Sverige.

I DL har riskerna för s.k. dataflykt uppmärksammats, dvs. att databehandlingen flyttas över från det egna landet till ett annat land för att undgå integritetsskyddslagstiftningen i hemlandet.[31] Mitt förslag till undantag från DL för att tillgodose yttrande- och informationsfriheten kan visserligen sägas öka riskerna för sådana åtgärder. Löpande text torde emellertid som framgått vanligtvis inte utgöra personregister, och även undantaget för register över meddelanden och användare gäller endast i den mån registret förs för yttrandefrihetsrättsliga syften.

Beträffande dataflödet i motsatt riktning finns inga särskilda regler i DL, och det anses tveksamt om DL över huvud taget är tillämplig på flödet av data från ett utländskt personregister som är tillgängligt via terminal i Sverige för svenska användare. Registret förs ju utom riket.[32]

Det är svårt att tänka sig att sådana gränsdragningar, baserade på var insamling fysiskt sker och var ett register fysiskt förs, kan fungera inom ramen för globalt tillgängliga tjänster för att söka, insamla, bevara och ta del av data. Frågor om skyddet för persondata övervägs dock i annan ordning (dir. 1995:91).

Här aktualiseras främst frågan om de straffsanktionerade ordningsreglerna i den förslagna särskilda lagen samt vissa bestämmelser om straffansvar i t.ex. brottsbalken kan tillämpas på dataflödet till Sverige från förmedlingstjänster som helt eller delvis bedrivs utanför riket.[33]

[31] Enligt 2 § fjärde stycket DL krävs licens, och eventuellt tillstånd, redan för att samla in personuppgifter, om avsikten är att de skall ingå i ett register. Härvid saknar det betydelse om databehandlingen av de insamlade uppgifterna skall ske i Sverige eller utomlands, och det krävs för vissa fall, som framgått av avsnitt 10.2.3, medgivande av Datainspektionen om uppgifterna skall lämnas ut för att databehandlas i utlandet (Kring/Wahlqvist, Datalagen, 1989, s. 28 och 79).

[32] Kring/Wahlqvist, a.a., s. 217.

[33] Detta är inte något nytt problem. Brottslig spridning av information mellan olika länder har sedan länge kunnat äga rum via t.ex. post och radiovågor. Det nya är att möjligheterna till spridning ökat i sådan omfattning att traditionell övervakning och kontroll för

Bestämmelserna i brottsbalken är som huvudregel inte territoriellt begränsade. Brott kan förövas var som helst, såvida inte särskild anledning till motsatt bedömning föreligger.[34] Beträffande specialstraffrätten är utgångspunkten i stället att gärningarna utgör brott bara om de har förövats på svenskt territorium. Detta gäller även yttrandefrihetsbrott enligt TF och YGL; jfr 13 kap. TF och 10 kap. YGL. Förutsättningarna för att ett brott skall anses vara begånget i Sverige har dock gjorts så vida att lagföring vanligtvis inte hindras av territoriella begränsningar.[35] Detsamma gäller föreskrifterna i 2 kap. BrB om när svensk domstol har kompetens att döma över ett visst brott.

Vad härefter beträffar de föreslagna ordningsreglerna i den särskilda lagen, om information till användare och förhindrande av fortsatt spridning av vissa typer av meddelanden, kan först konstateras att de endast har till syfte att skydda svenska intressen; svenska myndigheter kan naturligtvis inte agera världspolis på IT-området och det är uppenbart att svenska ordningsregler inte kan gälla för t.ex. amerikanska förmedlingstjänster knutna till Internet.

Detta innebär emellertid inte att de föreslagna reglerna alltid skall anses vara territoriellt begränsade till förmedlingstjänster som fysiskt finns i Sverige; regleringen avser tillhandahållande av information. Om exempelvis någon som har hemvist i Sverige, för att kringgå den föreslagna regleringen, flyttar sin förmedlingstjänst till datorer i ett annat land — t.ex. till ett s.k. Web-hotell — eller startar en förmedlingstjänst med användning av datorer utom riket men inriktar förmedlingstjänsten på svenska användare, bör den föreslagna lagen anses tillämplig. Att tjänsten har en sådan inriktning på svenska användare kan ta sig uttryck i bl.a. valen av språk för tjänsten (svenska) och ämnen för elektroniska konferenser (t.ex. lokalt betingade svenska diskussionsgrupper). Det kan också vara så att inläggen i konferenser m.m. helt präglas av svenska användare. Förutsättningarna kan dock variera i sådan grad att frågan bör överlämnas åt praxis.

I praktiken torde en sådan nationell begränsning knappast vålla svårigheter. Rent allmänt gäller att brott i ett land sällan blir kända i andra länder och att åtal mot personer som befinner sig utomlands sällan kan genomföras. Vidare torde svensk polis inte utan medgivande få vidta tjänsteåtgärder (t.ex. husrannsakan) med avseende på datorer

att förhindra missbruk vanligtvis inte är möjlig.

[34] Bland de gärningstyper som är av intresse i anknytning till elektroniska förmedlingstjänster kan nämnas att bestämmelserna om hets mot folkgrupp (16 kap. 8 § BrB) och barnpornografibrott (10 a §) inte torde vara territoriellt begränsade, medan motsatsen anses gälla beträffande olaga våldsskildring i (10 b §) och otillåtet förfarande med pornografisk bild (11 §). Tillämpningsområdet för bestämmelsen om uppvigling (16 kap. 5 § BrB) begränsas så att det för ansvar förutsätts att någon försöker förleda till *svensk* brottslig gärning, svikande av *svensk* medborgerlig skyldighet etc.

[35] Se vidare SOU 1992:110 s. 470 f.

i andra länder, och det finns regler om diskretionär åtalsprövning samt mot dubbelbestraffning.

11.8 Åtgärder i andra länder

Frågan om en reglering av förmedlingstjänster av internationell eller rent av global karaktär har funnits på dagordningen några år utan att några synbara resultat nåtts.

I USA har president Clinton nyligen skrivit under en mycket försenad och omdebatterad lag — Communications Decency Act of 1995, som är tillämplig på "Obscene, Harassing, and Wrongful Utilization of Telecommunications Facilities". Lagen gör det till ett federalt brott att skicka "oanständigt" material till personer under 18 år över nätverk av typ Internet. Eftersom lagen också gäller för meddelanden från utlandet torde även svenskar som gör t.ex. pornografi tillgängligt via Internet kunna straffas i USA. Påföljden är fängelse högst två år och böter upp till 100 000 US-dollar. Lagen berör även en del specifikt amerikanska yttrandefrihetsproblem i anslutning till de olika metoder som finns att censurera eller blockera delar av elektroniska förmedlingstjänster. I flera amerikanska delstater finns eller pågår arbete med lagstiftning kring förmedlingstjänster, bl.a. på skatteområdet.

Länder som har en restriktiv inställning till yttrandefrihet och politisk diskussion såsom Kina har enligt uppgift ålagt dem som tillhandahåller tjänster för förmedling av elektroniska meddelanden en skyldighet att inte tillåta användare att etablera kontakt med förmedlingstjänster som inte är "godkända".

Sedan den i Frankrike förbjudna boken Le Grand Secret, om president Mitterand, gjorts tillgänglig på Internet har intresset vaknat i Frankrike att försöka få till stånd en internationell reglering av gränsöverskridande förmedlingstjänster. Ett sådant initiativ avses i första hand föras fram inom EU.

Att sådana frågor redan har uppmärksammats i internationella fora framgår bl.a. av motiven till den nämnda Europarådsrekommendationen angående straff- och processrättsliga frågor med anknytning till IT, No. R (95) 13, där innehavarens/operatörens ansvar för en elektronisk anslagstavla nämns som ett viktigt område att följa upp.

11.9 Offentlighetsinsynen och de elektroniska förmedlingstjänsterna

Frågan om ADB-upptagningar som är tillgängliga för en myndighet via nät är att anse som allmänna handlingar och om de måste registreras enligt 15 kap. sekretesslagen (1980:100) har berörts i avsnitt 6.1. Jag

fann därvid att bestämmelsen i 2 kap. 6 § första stycket andra meningen TF borde förstås så att en teknisk möjlighet för myndigheten att hämta en ADB-upptagning från en databas som myndigheten helt saknar samröre med inte borde anses tillräcklig för att upptagningen skall anses inkommen till myndigheten.[36] Ett sådant resonemang är emellertid knappast hållbart beträffande upptagningar som en tjänsteman vid en myndighet verkligen tar del av, t.ex. när han "surfar på Internet". Tjänstemannen kan därvid dessutom t.ex. skriva ut en skärmbild eller i myndighetens dator lagra en upptagning han finner via nätet.

Handlingar anses vidare inkomna enligt 2 kap. 6 § TF oberoende av om de är av betydelse för myndighetens verksamhet. Frågan om ett meddelande med hänsyn till innehållet bör anses som allmän handling berörs emellertid i 2 kap. 4 § TF, där det föreskrivs att ett meddelande som är ställt personligen till den som innehar befattning vid myndighet anses som allmän handling, om handlingen gäller ärende eller annan fråga som ankommer på myndigheten och ej är avsedd för mottagaren endast som innehavare av annan ställning.

Traditionella handlingar som är privata anses inte vara inkomna och allmänna bara för att en tjänsteman har tagit med sig dem till sin arbetsplats,[37] och detsamma bör gälla beträffande privata upptagningar som tjänstemannen medför till sin arbetsplats, t.ex. genom att ta med sin bärbara dator. Detta bör också gälla om tjänstemannen i stället "surfar på nätet" och därvid, med myndighetens tekniska hjälpmedel men helt utan samband med tjänsteutövningen, för "privata" upptagningar till myndighetens dator; jfr att ett privatbrev skrivs på myndighetens skrivmaskin eller kommer in till myndigheten.

En mer svårbedömd situation uppkommer om en tjänsteman som arbetar med myndighetens datafrågor"surfar" i tjänsten, t.ex. för att från teknisk synpunkt studera den grafiska utformningen av olika s.k. Web-sidor. Han är därvid ointresserade av den sakinformation som lämnas på de sidor han studerar, och denna information är helt ovidkommande för myndigheten. Det kan därför ifrågasättas om sådant material utgör handlingar i TF:s bemärkelse när huvudsyftet är att förmedla rent estetiska intryck.[38] Och om inte tjänstemannen väljer att lagra eller skriva ut det material han studerar, är det enligt min mening knappast realistiskt att säga att materialet är "inkommet" till myndigheten. Rättsläget är emellertid oklart.

[36] Med hänsyn till utformningen av 2 kap. 3 § andra stycket första meningen TF är sådana upptagningar dock att anse som "förvarade" hos myndigheten (jfr Bohlin, Allmänna handlingar, s. 81).

[37] Bohlin, Allmänna handlingar, s. 120, med hänvisningar.

[38] Bohlin, a.a., s. 63.

Som allmän handling anses inte heller upptagningar som omfattas av den s.k. biblioteksregeln (2 kap. 11 § TF).[39]

Skulle åtkomst via nät till elektroniska förmedlingstjänster likväl leda till att upptagningar i stor omfattning blir att anse som allmänna, bör nuvarande reglering ändå kunna fungera i avvaktan på den översyn av 2 kap. TF som pågår i annan ordning (dir. 1995:91).[40] Är handlingar av ringa betydelse[41] för verksamheten vid myndigheten får detta beaktas inom ramen för reglerna om registrering och gallring av handlingar.

Enligt 15 kap. 1 § första stycket sekretesslagen (1980:100) behöver handlingar som uppenbart är av ringa betydelse varken registreras eller hållas ordnade på särskilt sätt, och handlingar som är av betydelse men som inte är sekretessbelagda behöver endast hållas ordnade så att det utan svårighet kan fastställas om handling har kommit in.[42] Krävs registrering i något fall bör detta enkelt kunna ske genom att tjänstemannen t.ex. överlämnar en utskrift till registrator.

Myndigheterna får, i enlighet med Riksarkivets allmänna gallringsregler[43], gallra handlingar som är av tillfällig eller ringa betydelse för myndighetens verksamhet. Gallring får ske vid tidpunkt eller med frist som fastställs av myndigheten själv. Exempel på handlingar som kan komma i fråga för gallring i enlighet med dessa regler är handlingar som inkommit för kännedom och som inte har lett till några åtgärder hos myndigheten och som inte heller har tillfört något ärende en sakuppgift.

[39] Bestämmelsen torde dock vara tillämplig endast om handlingarna har samlats och ordnats på sådant sätt att samlingen enligt vanligt språkbruk är att betrakta som ett bibliotek (prop. 1975/76:160 s. 180 och Bohlin, a.a., s. 220).

[40] Det kan härvid bli svårt att från offentlighetssynpunkt finna några tydliga skillnader mellan åtkomst via arbetsgivarens informationssystem och tjänstemannens hemdator. Det kan t.ex. göras tekniskt möjligt för en tjänsteman — även om så knappast sker — att med myndighetens tekniska hjälpmedel och telenätet logga in på tjänstemannens hemdator och, med myndighetens dator som terminal, styr hemdatorn så att han får tillgång till en elektronisk förmedlingstjänst.

[41] I Statsrådsberedningens promemoria Registrering av allmänna handlingar hos departementen (reviderad den 26 februari 1990), ges bl.a. följande exempel på handlingar som normalt uppenbarligen är av ringa betydelse. Pressklipp, reklamtryck, statistiska meddelanden, cirkulär som bara indirekt eller i någon mån berör departementens verksamhet, verksamhetsberättelser, årsredovisningar och annan allmän information som tillställs departementet utan att det finns skyldighet att göra det och utan att materialet hör till något ärende, sådana kopior av myndigheters yttranden m.m. som sänts över bara för kännedom och som inte kan användas som allmänt underlag för regerings- eller departementsbeslut och inte heller på annat sätt kan vara till nytta för departementet, kopior av brev från enskilda till olika myndigheter i de fall där kopiorna bara sänts över för kännedom och anonyma skrivelser.

[42] Sådana ordnade bevaringsmöjligheter bör kunna skapas med stöd av IT.

[43] Riksarkivets föreskrifter och allmänna råd om gallring av handlingar av tillfällig eller ringa betydelse (RA-FS 1991:6).

12 Straffrättsliga och straffprocessuella frågor

12.1 Utgångspunkter

Användningen av IT har ökat riskerna för otillåten spridning av information och begränsat möjligheterna att utreda och lagföra brott.[1] Mina förslag syftar därför till att delvis återställa möjligheterna att, med rimlig resursåtgång, kunna ingripa mot otillåtna förfaranden där missbruket berör elektroniska förmedlingstjänster i stället för traditionella medier.

Den naturliga utgångspunkten är, som framhållits i avsnitt 11.3.3, att ansvaret för brott i första hand bör bäras av den som utför eller ligger bakom den aktuella åtgärden. För att underlätta efterforskning av denne har jag övervägt regler om bl.a. registrering av förmedlingstjänster och användare samt om bevaring av meddelanden. Det har emellertid visat sig att en sådan reglering för närvarande inte är något realistiskt alternativ; se vidare avsnitt 11.4.3 och 11.4.7.

Däremot har jag föreslagit en föreskrift om att den som tillhandahåller en elektroniska förmedlingstjänst skall ha sådan uppsikt över tjänsten som är nödvändig med hänsyn till omfattningen och inriktningen av verksamheten. Jag har också föreslagit att den som tillhandahåller tjänsten vid straffansvar skall vara skyldig att i viss utsträckning förhindra fortsatt spridning av elektroniska meddelanden med brottsligt eller annars oacceptabelt innehåll. Härigenom ges ett grundläggande skydd mot missbruk av elektroniska förmedlingstjänster. Förslaget att förmedlaren skall underrätta dem som ansluter sig om vem som är ansvarig för tjänsten bör också kunna underlätta åtgärder mot oseriösa företeelser på området.

Straffansvar kan således komma i fråga dels för användare som ligger bakom ett missbruk, dels för ansvariga för förmedlingstjänster och dennes biträden som åsidosätter de ordningsregler som jag har föreslagit. Beträffande ansvariga för förmedlingstjänster uppkommer —

[1] En följd av datoriseringen på 1970-talet var att möjligheterna att utkräva personligt ansvar begränsades genom att IT-rutiner infördes där den spårbarhet som förelåg i traditionell miljö endast delvis vidmakthölls. Den kultur som vuxit fram bland användare av elektroniska förmedlingstjänster har inneburit ytterligare ett steg i riktning mot en avidentifiering av aktörerna.

när någon annan missbrukar tjänsten — dessutom frågan om ansvar för osjälvständiga brottsformer såsom medverkan till brott.

12.2 Ansvar för användare vid missbruk av elektroniska förmedlingstjänster

Utgångspunkten är som sagt att straffansvaret i första hand bör vila på de användare som missbrukar en elektronisk förmedlingstjänst. Frågan är då om regleringen i brottsbalken är anpassad till brottslighet som begås via sådana tjänster. I det följande behandlas denna fråga med utgångspunkt i de typfall som beskrivits i avsnitt 10.2.1.[2]

12.2.1 Uppvigling, hets mot folkgrupp, barnpornografibrott, m.m.

De objektiva rekvisiten för *uppvigling* (16 kap. 5 § brottsbalken) hindrar inte i sig en lagföring av förfaranden knutna till elektroniska förmedlingstjänster, och bestämmelsen har givits en tidig fullbordanspunkt. I ett avseende finns emellertid en skillnad mellan spridning som sker i skrift respektive elektroniskt. Uppvigling genom spridning av "skrift" är fullbordad redan genom att skriften "utlämnas för spridning".[3] Begreppet skrift torde dock inte omfatta elektroniska meddelanden. Denna skillnad bör undanröjas.

De objektiva rekvisiten för *hets mot folkgrupp* (16 kap. 8 § brottsbalken) hindrar inte heller en lagföring av elektroniska förfaranden, och kravet att meddelande som uttrycker hot eller missaktning mot folkgrupp på grund av ras eller dylikt "sprids", är lågt ställt.

Hets mot folkgrupp är emellertid inte kriminaliserat på försöksstadiet. Inte heller vid *barnpornografibrott, olaga våldsskildring och förledande av ungdom* (16 kap. 10 a, 10 b och 12 §§ brottsbalken) är försök till brott straffbelagt.[4]

När någon i spridningssyfte har sänt ett meddelande med sådant innehåll som avses i de nu nämnda bestämmelserna till en elektronisk förmedlingstjänst, ligger det vanligtvis utanför avsändarens kontroll hur omfattande spridningen blir. Gärningsmannen har genom att avsända meddelandet fullgjort allt för att ett brott skall komma till stånd. Så

[2] De generella straffrättsliga frågorna på IT-området faller dock utanför mitt uppdrag; jfr bl.a. SOU 1983:50, prop. 1985/86:65 och SOU 1992:110.

[3] Enligt Straffrättskommittén var det önskvärt att paragrafen kunde tillämpas även om skriften hejdats av postverket innan spridning har skett; jfr bestämmelsen i 23 kap. 1 § BrB om ansvar för försök till brott.

[4] Gärningar som avses i 16 kap. 11 § andra meningen brottsbalken fullbordas redan när en bild lämnas för befordran (Beckman m.fl., Brottsbalken II, 6 u., s. 289 och Jareborg, Brotten III, 2 u., s. 139).

snart meddelandet finns tillgängligt elektroniskt kan det sekundsnabbt föras vidare till andra förmedlingstjänster, och bevissvårigheter framträder när det skall avgöras vilken spridning som i realiteten har skett.[5] En möjlighet är att meddelandet har stoppats just med avseende på den förmedlingstjänst som avsändaren dirigerat det till, men i stället omdirigerats till en annan sådan tjänst.[6] Elektronisk överföring av berörda meddelanden skiljer sig därmed i sådan mån från traditionella förfaranden att redan avsändandet till en elektronisk förmedlingstjänst bör straffbeläggas.

Jag föreslår därför en bestämmelse enligt vilken den som sänder ett elektroniskt meddelande med sådant innehåll som avses i 16 kap. 5, 8, 10 a, 10 b eller 12 § brottsbalken till en elektronisk förmedlingstjänst, med uppsåt att utföra brott som sägs i någon av dessa bestämmelser, skall dömas för försök till sådant brott, om han inte kan dömas för fullbordat brott. Ansvar inträder därmed även om meddelandet inte förs in, eller om det avförs innan spridning har skett. Det vore i och för sig möjligt att placera bestämmelsen i den särskilda lag jag föreslår för elektroniska förmedlingstjänster. Eftersom bestämmelsen sakligt sett har ett mycket nära samband med övriga regler i 16 kap. brottsbalken är det dock naturligt att placera den där; jfr regleringen i 4 kap. 9 b § brottsbalken (16 kap. 17 a § förslaget till lag om ändring i brottsbalken).[7]

Vissa tolkningsfrågor som aktualiseras i anknytning till dessa bestämmelser bör också beröras.

Bestämmelsen i 16 kap. 10 a § brottsbalken om barnpornografibrott innefattar alla slag av bilder med barnpornografiskt motiv, och modern teknik berörs i sammanhanget.[8] *Begreppet "bild"* förekommer emellertid också i bestämmelserna om olaga våldsskildring, otillåtet förfarande med pornografisk bild och förledande av ungdom. Frågan är hur dessa bestämmelser bör tolkas i anknytning till nya medier.

Vad som möjligen kan föranleda tvekan är vissa uttalanden i lagmotiven. I anknytning till 16 kap. 12 § brottsbalken har departementschefen å ena sidan anfört att alla slags bilder omfattas, vare sig de har framställts genom tryckpress eller på annat sätt, å andra sidan att

[5] En oriktig invändning att ett meddelande av sådan art inte har lästs av någon och inte heller annars har nått en sådan spridning som krävs för ansvar, torde ofta kunna motbevisas genom innehållet i loggfiler m.m. Däremot kan det ofta vara svårt att fastställa vilken vidare spridning som skett därefter.

[6] Det kan närmast vara en slump om ett elektroniskt meddelande hindras, t.ex. av tekniska fel vid överföringen eller vid stickprovskontroller där en systemansvarig avför meddelanden innan vidare spridning har skett.

[7] Härigenom undviks de komplicerade konkurrensfrågor som följer med en specialstraffrättslig reglering. En annan fördel med en placering i 16 kap. brottsbalken är att frågan om påföljd kan regleras utifrån straffskalorna i huvudbestämmelserna.

[8] Jareborg uttalar att alla tänkbara förfaranden varigenom ett bildinnehåll förmedlas till eller görs tillgängligt innefattas samt nämner förevisning genom bl.a. optisk anordning (Jareborg, Brotten III, 2 u., s. 139).

bestämmelsen omfattar endast sådana "föremål som kan hänföras till avbildningar".[9] Det kan ifrågasättas om data ryms under begreppet föremål.[10]

Enligt min mening är det dock uppenbart att begreppet "bild" måste anses omfatta också digitala bilder — begreppet måste antas ha samma innebörd i hela 16 kap. brottsbalken.

En annan fråga är i vilken mån straffrättsligt ansvar kan komma i fråga vid *förevisning* av t.ex. pornografiska bilder *via* sådana allmänt tillgängliga *"elektroniska platser"*, som ger förutsättningar för en betydligt mer omfattande spridning än vad som möjliggörs vid en vanlig allmän plats.

Bestämmelsen i 16 kap. 11 § första meningen brottsbalken synes avse endast traditionella fysiska utrymmen, och att utsträcka regelns tillämplighet till visning via elektroniska förmedlingstjänster vore enligt min mening att gå för långt. Man skulle möjligen kunna ställa krav på varningstexter så att ingen mot sin vilja råkade ut för att behöva se pornografiska bilder. Det finns emellertid programvara att installera på den egna datorn som förhindrar uppkoppling till kända platser på Internet där pornografi förekommer. (Surf Watch, Net Nanny m.fl.). Däremot kan naturligtvis regeln i paragrafens andra mening bli tillämplig om någon skickar pornografiska bilder i form av elektronisk post till enskilda användare.

12.2.2 Ansvar enligt brottsbalken för brott mot en viss person

I den mån brottslig informationsspridning via elektroniska förmedlingstjänster riktas mot en viss person aktualiseras ansvar för olaga hot, ofredande, förtal och förolämpning (4 kap. 5 och 7 §§ samt 5 kap. 1 och 3 §§ brottsbalken), inte bestämmelserna om uppvigling eller hets mot folkgrupp. I dessa delar är det inte nödvändigt med någon lagändring med anledning av elektroniska förmedlingstjänster.[11]

Det bör härvid uppmärksammas att den som skickar oönskad information till en viss person — oönskad på grund av innehållet eller mängden — därvid kan göra sig skyldig till ofredande på samma sätt som den som utnyttjar telefon eller post på ett hänsynslöst sätt. Som exempel kan nämnas den som själv eller i samråd med andra "fyller" en användares elektroniska brevlåda så att tjänsten inte längre kan

[9] Beckman m.fl., Brottsbalken II, 6 u., s. 287 f.

[10] SOU 1992:110, bl.a. s. 155 f. och 209 f.

[11] Jag vill emellertid erinra om Datastraffrättsutredningens förslag till ändring i 4 kap. 5 § brottsbalken, för att också hot som riktas mot data, inte mot "egendom", klart skall innefattas.

användas. Därvid torde också ansvar för egenmäktigt förfarande kunna komma i fråga.[12]

12.2.3 Narkotikabrott genom utbud via elektroniska förmedlingstjänster

Den som *bjuder ut narkotika* kan i allmänhet dömas till ansvar genom att de osjälvständiga brottsformerna är kriminaliserade vid överlåtelse av narkotika. Enligt motiven till 1 § 5 narkotikastrafflagen (1968:64), där ansvar föreskrivs för den som olovligen bjuder ut narkotika till försäljning, har det dock ansetts nödvändigt att ge upp kravet på att det alltid i det konkreta fallet skall kunna visas att förfaranden av aktuellt slag främjat ett bestämt narkotikabrott.[13]

Det bör således finnas visst utrymme för straffansvar för den som genom elektroniska meddelanden bjuder ut narkotika eller annars via elektroniska förmedlingstjänster främjar narkotikahandel. Det skall emellertid kunna visas att förfarandet haft eller kunnat få anknytning till transaktioner som utgör narkotikahandel.[14]

12.2.4 Skadegörande programkod, m.m.

De särskilda risker som *datavirus* och annan skadegörande programkod innebär vid elektronisk kommunikation har berörts av Datastraffrätts-utredningen, som föreslagit särskilda bestämmelser om straff för den som tillverkar och sprider sådana program.[15] Förslaget övervägs för närvarande inom Justitiedepartementet. Bestämmelserna om skadegörelse, undertryckande av urkund och dataintrång (12 kap. 1 § och 14 kap. 4 § brottsbalken samt 21 § DL) torde dock, beroende på omständigheterna i det enskilda fallet, kunna aktualiseras också med avseende på skadegörande programkod som en användare för in eller annars sprider via en elektronisk förmedlingstjänst.[16]

[12] Se vidare Jareborg, Brotten II, 2 u., s. 122.

[13] I motiven till bestämmelsen sägs att förmedling av kontakter mellan köpare och säljare i många fall kan vara att bedöma som medhjälp antingen till överlåtelse eller till förvärv av narkotika, men att det i många fall har visat sig svårt att bevisa att handhavandet lett till ett visst bestämt brott. Eftersom "annan sådan åtgärd" också är kriminaliserad torde det vara tillräckligt att förmedlaren har gjort det möjligt att en kontrahent i handeln får kännedom om den andres bud. Det bör dock inte, vid en strikt tolkning av ordalydelsen, fällas till ansvar enligt 1 § 5 narkotikastrafflagen om den misstänkte endast i ett enstaka fall har sammanfört en köpare och en säljare (Hoflund, Olle, Narkotikabrotten, 1987, s. 49 f.).

[14] Prop. 1982/83:141 s. 34; jfr Hoflund, Olle, Narkotikabrotten, 1987, s. 47 f.

[15] SOU 1992:110 s. 214 f.

[16] Risken för spridning av datavirus har ökat genom det nya programmeringsspråket Java samt möjligheten att översända makron för ordbehandlingsprogrammet Word i vanliga textfiler.

12.2.5 Upphovsrättsligt skydd

De nya förutsättningar för den upphovsrättsliga regleringen som användningen av elektroniska förmedlingstjänster har fört med sig är av sådan grundläggande och generell karaktär att rättsfrågorna inte kan genomlysas i detta begränsade sammanhang. Detta gäller inte bara skyddet för datorprogram utan också för t.ex. text, bild och musik i digital form. Utvecklingen aktualiserar behovet av en upphovsrättslig reglering som tar sikte på dessa nya företeelser och undanröjer tolkningsfrågor och luckor i lagen. Detsamma gäller för sådant offentligt framförande och sådan spridning till allmänheten av verk som sker via elektroniska förmedlingstjänster. Jag återkommer i avsnitt 12.3 till frågan om straffansvar för den som tillhandahåller en elektronisk förmedlingstjänst.

12.2.6 Meddelanden vilkas innehåll är ägnat att användas vid brott[17]

Som redan berörts innehåller vissa elektroniska förmedlingstjänster dels *"elektroniska brottsverktyg"*, t.ex. datorprogram för att kringgå behörighetskontrollsystem, hemliga tillträdeskoder och telefonkorts- och kontokortsnummer, dels *närmare beskrivningar av brottsliga förfaringssätt*, t.ex. hur telebedrägerier genomförs — i vissa fall förenade med uttryckliga uppmaningar till brott.

Föreskrifterna i 23 kap. brottsbalken om s.k. osjälvständiga brottsformer utvidgar det straffbara området utanför de gränser som dras av brottsbeskrivningarna i de särskilda straffbuden. Frågan är då om användare kan dömas till ansvar för förberedelse eller stämpling till brott vid förfaranden i anknytning till elektroniska förmedlingstjänster.

Förberedelse till brott består — såvitt här är av intresse — i att anskaffa, förfärdiga, lämna, motta, förvara, fortskaffa eller ta annan dylik befattning med vissa objekt. Lagregeln avser emellertid traditionella fysiska objekt såsom gift, sprängämne, vapen, dyrk, förfalskningsverktyg eller annat sådant hjälpmedel. Datastraffrättsutredningen har föreslagit en reglering av förberedelse som innefattar data.[18] Regleringen övervägs nu av utredningen rörande vissa straffrättsliga frågor (dir. 1994:39). Jag konstaterar därför endast att ansvar för "elektronisk förberedelse" till brott torde förutsätta en lagändring.

Vad härefter beträffar *stämpling* enligt 23 kap. 2 § andra stycket brottsbalken, genom att *söka anstifta* annan till brott, kan konstateras

[17] Jfr 5 § förslaget till lag om tjänster för förmedling av elektroniska meddelanden.

[18] Se vidare förslaget till en ny 23 kap. 2 a § BrB, SOU 1992:110 s. 32, 200 f., 325 f. och 603 f.; jfr Datastraffrättsutredningens förslag i 14 kap. 19 § BrB att kriminalisera missbruk av lösenord.

att det endast är ett mindre antal brott av grövre karaktär som är straffbara redan på detta stadium. Att söka anstifta till brott innebär vidare att träda i förbindelse med viss eller vissa personer, till skillnad från uppvigling, som innebär att man vänder sig till allmänheten. Vidare måste denna form av stämpling, för att vara straffbar, ske med direkt uppsåt att det ifrågavarande brottet skall komma till stånd.[19]

Utrymmet för straffansvar, för användare som sänder in ett elektroniskt meddelande som kan sägas söka anstifta till brott, är således synnerligen begränsat. Sådana meddelanden är vanligtvis riktade till allmänheten, och det kan ofta ifrågasättas om "anstiftaren" verkligen har uppsåt att brottet skall komma till stånd.

12.3 Straffansvar för den som tillhandahåller en elektronisk förmedlingstjänst

12.3.1 Allmänt

I detta sammanhang aktualiseras också vilket straffrättsligt ansvar den som tillhandahåller en elektronisk förmedlingstjänst har för meddelanden som användare sänder in till tjänsten.

När den som tillhandahåller tjänsten genom eget *aktivt handlande* gör meddelanden med brottsligt innehåll tillgängliga, t.ex. genom att föra in sådana meddelande i en allmänt tillgänglig area, kan han bli att bedöma som gärningsman under förutsättning att uppsåt föreligger.

Av betydelse från praktisk utgångspunkt är emellertid i första hand frågan om en förmedlare som förhåller sig passiv kan dömas till ansvar enligt brottsbalken eller annan tillämplig lag, dvs. om han kan göra sig skyldig till brott genom *underlåtenhet*.[20]

Ansvar för medverkan genom underlåtenhet kan aktualiseras såväl beträffande fullbordat brott som stämpling till brott.[21] För ansvar krävs dels att medhjälparen är i s.k. garantställning, dels att han med sin passivitet underlättar den andres gärning.[22] Med garantställning menas att den underlåtande skall inta en ställning som gör det motiverat att

[19] Beckman m.fl., Brottsbalken II, 6 u., s. 605.

[20] Det kan inte uteslutas att en förmedlare kan göras ansvarig som gärningsman. Som exempel kan nämnas den bestämmelse som berörts i avsnitt 12.2.3 enligt vilken ansvar enligt 1 § 5 narkotikastrafflagen kan komma i fråga redan om en "förmedlare" har gjort det möjligt att en kontrahent i handeln får kännedom om den andres bud. Samtidigt är stämpling till narkotikabrott kriminaliserad.

[21] Medverkan till brott är generellt straffbelagt, dvs. medverkan till stämpling är också kriminaliserad, förutsatt att brottsformen stämpling är straffbelagd i det aktuella fallet (Jareborg, Brotten I, 2 u., s. 63 f.).

[22] Jareborg, Straffrättens ansvarslära, 1994, s. 127. Jfr Strahl, Allmän straffrätt i vad angår brotten, 1976, s. 248 och 336 f.

begära mer av honom än av andra att han skall vara verksam för att avvärja en sådan effekt som den inträffade.[23]

De skyldigheter jag har föreslagit för den som tillhandahåller tjänsten och den som på hans uppdrag har uppsikt över tjänsten (se 3 och 5 §§ förslaget till lag om elektroniska förmedlingstjänster) ger dem en sådan garantställning, och en underlåtenhet att agera beträffande meddelanden som innefattar t.ex. uppvigling eller hets mot folkgrupp kan te sig lika straffvärd som främjande av gärningen genom handling.[24] Om den som tillhandahåller en elektronisk förmedlingstjänst eller den som på hans uppdrag har tillsyn över tjänsten får klart för sig att tjänsten används för att sprida viss information av brottslig karaktär men underlåter att hindra en fortsatt sådan användning av tjänsten kan han alltså ådra sig eget straffansvar för de meddelanden som sprids. Därigenom bör kunna undvikas att en ansvarig för en förmedlingstjänst som passivt ser på när brottslig spridning äger rum går fri medan den som gör något, om än litet, kan dömas till ansvar.[25]

12.3.2 Tillämpningen av enskilda straffbestämmelser

Här tar jag endast upp några frågor som har väckts rörande förutsättningarna för att tillämpa enskilda straffbestämmelser på ansvariga för elektroniska förmedlingstjänster.[26]

Beträffande uppvigling torde rekvisitet "söker förleda" innefatta ett krav på direkt uppsåt, dvs. att det för ansvar — utöver kännedom om förhållandena — krävs en viljeriktning, i detta fall ett syfte att förleda en allmänhet till brott eller dylikt.[27] Endast i undantagsfall torde den verksamhet ansvariga för förmedlingstjänster bedriver ha ett sådant syfte.

Angående hets mot folkgrupp och huvuddelen av övriga straffbestämmelser som aktualiseras på området finns visserligen inget krav på direkt uppsåt, och i den bemärkelsen ligger ett straffansvar närmare för den som är ansvarig för en förmedlingstjänst. En annan sak är att strömmen av meddelanden i praktiken vanligtvis har en sådan omfattning att det med fog kan ifrågasättas om den som är ansvarig för

[23] Strahl, a.a., s. 323.

[24] På den subjektiva sidan torde krävas att förmedlaren har uppsåt att medverka till avsändarens spridning, att han förstår, på sätt uppsåtsläran anger, att gärningen kommer till stånd om han inte ingriper avvärjande samt att hans uppsåt omfattar att han intar en garantställning.

[25] Se vidare HD:s uttalanden i den ovan berörda domen angående spridning av datorprogram via elektroniska anslagstavlor (avsnitt 10.2.1 under rubriken "Upphovsrättsligt skyddat material").

[26] Frågan om utformningen av bestämmelserna i brottsbalken av bl.a. medverkan till brott övervägs av utredningen om vissa straffrättsliga frågor (dir. 1994:39).

[27] Beckman m.fl., Brottsbalken II, 6 u., s. 248 med hänvisning till s. 246, Jareborg, Brotten III, 2 u., s. 130 och Strahl, Allmän straffrätt i vad angår brotten, 1976, s. 107.

tjänsten har sådana insikter om vad som pågår att det finns utrymme för ansvar för uppsåtligt brott.[28]

Diskrimineringsombudsmannen har i en skrivelse till Justitiedepartementet aktualiserat bl.a. frågan om den som tillhandahåller en elektronisk anslagstavla, genom detta tillhandahållande, kan sägas "hota" på sätt som sägs i 16 kap. 8 § brottsbalken, för den händelse en användare av förmedlingstjänsten har tillfört ett meddelande vars innehåll utgör hets mot folkgrupp.

Som framgått är utrymmet för ansvar beträffande medverkan genom underlåtenhet begränsat, och straffbestämmelsens krav på uppsåt måste uppfyllas av den medverkande själv, i detta fall den som är ansvarig för förmedlingstjänsten. Han behöver emellertid inte själv hota eller uttrycka missaktning för en grupp av personer. Det räcker att hans uppsåt omfattar att avsändaren hotar.[29]

Här bör också nämnas att HD i den ovan berörda domen angående spridning av datorprogram via elektroniska anslagstavlor funnit att ansvar för intrång i upphovsrätt enligt 2 § upphovsrättslagen förutsätter någon form av aktivt handlande.[30] Av domen framgår vidare att framställning av exemplar genom elektronisk överföring innefattas i upphovsmannens ensamrätt.

Ansvar för *häleri* kan komma ifråga för den som otillbörligen främjar möjligheterna för annan att tillgodogöra sig egendom som härrör från brottsligt förvärv (9 kap. 6 § BrB). För straffansvar enligt denna bestämmelse fordras att gärningen i det enskilda fallet gynnat någons möjligheter att tillgodogöra sig egendomen eller dess värde. Det räcker inte att förfarandet typiskt sett varit ägnat att öka möjligheterna för någon att dra nytta av det brottsliga förvärvet. Min grundinställning är som redan framhållits att samma förhållanden bör råda i "cyberspace" som i den verkliga världen. Skulle då en ansvarig utgivare kunna straffas om han i tidningens annonsspalter medvetet tog in annonser under rubriken "stöldgods till salu"? Frågan om möjligheten att vid sidan av TF ingripa mot brott genom tryckt skrift har varit under bedömning i bl a rättsfallet NJA 1979 s. 602. Utan hinder av regleringen i TF fälldes den som i tidningsföretag haft den faktiska bestämmanderätten i fråga om införandet av annonser i företagens tidningar till ansvar för koppleri genom att tillåta annonser vari prostituerade utbjöd sina tjänster. Han ansågs därigenom ha främjat annans otuktiga levnadssätt (6 kap 7 § första stycket BrB i dess dåvarande lydelse).

[28] Jfr dock att ansvar för brott i vissa fall kan aktualiseras redan till följd av oaktsamhet.

[29] Ansvar för hets mot folkgrupp förutsätter inte heller att någon själv gör ett uttalande — det är tillräckligt att sprida vad man hört av annan (Beckman m.fl., Brottsbalken II, 6 u., s. 263 och Jareborg, Brotten III, 2 u., s. 134.).

[30] Se vidare avsnitt 10.2.1 under rubriken "Upphovsrättsligt skyddat material".

Den som är ansvarig för en elektronisk förmedlingstjänst torde på motsvarande sätt vid vetskap om förhållandet kunna fällas till ansvar för häleri i enskilda fall, oberoende av om publiceringen sker i ett grundlagsskyddat medium. Det behövs alltså ingen särskild reglering för att komma tillrätta med missbruk av elektroniska förmedlingstjänster för annonsering om stöldgods, prostitution o.dyl (jfr 5 § förslaget till lag om elektroniska förmedlingstjänster).

12.3.3 Skyldigheter för den som tillhandahåller tjänsten och skyddet mot intrång i information, m.m.

Mitt förslag till lag om elektroniska förmedlingstjänster innebär att den som tillhandahåller tjänsten åläggs att förhindra att brottsliga eller annars oacceptabla meddelanden sprids (5 och 6 §§ förslaget till lag om elektroniska förmedlingstjänster). Jag har redan i avsnitt 11.4.5 tagit upp frågan om den som tillhandahåller en förmedlingstjänst, i syfte att fullgöra de åligganden som följer av den föreslagna lagen, har rätt att läsa alla meddelanden som förmedlas via den tjänst han tillhandahåller. Här är främst den straffrättsliga regleringen av intresse.[31]

Bestämmelserna om brytande av telehemlighet, olovlig avlyssning och dataintrång i 4 kap. 8 och 9 a §§ BrB samt 21 § DL föreskriver straffansvar för den som "olovligen" bereder sig tillgång till information.

Bestämmelsen om brytande av telehemlighet omfattar endast meddelanden som ett post- eller telebefordringsföretag förmedlar som telemeddelande. Med post- och telebefordringsföretag avses företag som på affärsmässiga grunder huvudsakligen förmedlar information — meddelanden i form av postförsändelser och olika former av telemeddelanden — som andra lämnar för distribution.[32] Bestämmelsen torde således kunna bli tillämplig också på distribution via elektroniska förmedlingstjänster.[33]

Ansvar för olovlig avlyssning kommer i fråga endast vid avlyssning eller upptagning med tekniskt hjälpmedel av tal i enrum, samtal mellan andra, etc. Data, text och bild skyddas inte. Denna paragraf är därför knappast av intresse i anknytning till elektroniska förmedlingstjänster.

Bestämmelsen om dataintrång avser emellertid upptagningar för automatisk databehandling. Med sådan upptagning avses även uppgifter

[31] Skydd mot intrång i information föreskrivs dock i såväl internationella överenskommelser som i grundlag och vanlig lag; se vidare t.ex. prop. 1994/95:227 s. 8 f.

[32] Prop. 1992/93:200 s. 161 f.

[33] Jfr 24 § telelagen där det anges att ett telemeddelande får avlyssnas i televerksamhet endast i den utsträckning som det är nödvändigt för att verksamheten skall kunna drivas. Härmed avses den tekniska avlyssning som är nödvändig för att kontrollera telesystemets funktion i skilda hänseenden (prop. 1992/93:200 s. 309).

som är under befordran via elektroniskt eller annat liknande hjälpmedel för att användas för automatisk databehandling.[34]

Bestämmelserna om straffansvar för intrång i information har inte anpassats till utvecklingen på IT-området.[35] Rättsläget är delvis oklart. Frågan är när den som tillhandahåller en elektronisk förmedlingstjänst får anses ha förfarit "olovligen" enligt någon av de berörda straffbestämmelserna.

Användningen av elektroniska förmedlingstjänster utgörs till stor del av sådana tillämpningar där de elektroniska meddelandena blir omedelbart tillgängliga för alla användare av den elektroniska förmedlingstjänsten. Den som tillhandahåller tjänsten har därvid, redan på grund av denna allmänna åtkomst, rätt att ta del av de elektroniska meddelandena.

Motsatsen torde vanligtvis gälla för e-post, dvs. meddelanden som är avsedda bara för viss eller vissa användare.[36] Här kan en jämförelse med traditionella tillslutna rum, förvar, kuvert etc. underlätta förståelsen. Fyller en rutin motsvarande funktion som distribution av vanliga brev, eller förvaring av brev i t.ex. lådor som bara "mottagaren" får öppna, torde en åtgärd varigenom den som tillhandahåller en förmedlingstjänst tar del av innehållet vara att anse som "olovlig", om inte annat har överenskommits. I praktiken bör frågan kunna klargöras vid de kontakter som tas i samband med att användare bereds tillgång till en förmedlingstjänst.

Som framgått av avsnitt 11.4.5 skall skyldigheten enligt den särskilda lagen att förhindra fortsatt spridning av vissa meddelanden gälla också beträffande meddelanden i slutna diskussionsgrupper ock liknande. Den särskilda lagen får i denna del anses innebära att de föreskrivna skyldigheterna för den som tillhandahåller tjänsten medför att han inte "olovligen" tränger in i sådan information.

Som framgått gäller denna laga befogenhet emellertid inte e-post. Beträffande sådana meddelanden kan dock behöva vidtas administrativa åtgärder. Enligt min genomgång i avsnitt 11.6 kan härvid — utöver de

[34] Telelagens (25 och 29 §§) och sekretesslagens (9 kap. 8 § och 14 kap. 2 §) bestämmelser ger i förening med straffbestämmelsen om brott mot tystnadsplikt (20 kap. 3 § BrB) också visst skydd för telekommunikationer. — Meddelanden som befordras via radio skyddas inte av bestämmelserna om dataintrång och brytande av telehemlighet. Oavsiktlig spridning av uppgifter via etern, t.ex. i form av strålning från bildskärmar, s.k. röjande signaler, synes också falla utanför straffskyddet; se vidare SOU 1992:110 s. 163 f. Bestämmelsen om olovlig avlyssning innefattar emellertid upptagning och avlyssning såväl genom direkt användning av en mikrofon för att uppfånga vad som sägs i t.ex. ett rum (en slags spridning via etern) som genom att uppsnappa trådbundna signaler, t.ex. samtal via snabbtelefoner.

[35] Se dock Datastraffrättsutredningens förslag att föra samman denna reglering till en paragraf och att IT-anpassa regleringen (SOU 1992:110 s. 175 f.).

[36] Jag syftar härvid på sådan användning som motsvarar traditionella brev som postas till en eller ett par mottagare, inte på de distributionslistor som utgör ett medel för "gruppkommunikation", genom att meddelanden sänds vidare som elektronisk post till dem som upptas i listan.

berörda straffstadgandena — aktualiseras bestämmelser i bl.a. telelagen om förbud mot att "avlyssna" telemeddelanden utöver vad som är "nödvändigt för att verksamheten skall kunna drivas" (24 §), om tystnadsplikt (25 och 26 §§) och om att lämna ut vissa uppgifter (27 §); jfr 10 och 11 §§ postlagen (1993:1684) angående obeställbara försändelser. Till detta kommer att det enligt 27 kap. 19 § rättegångsbalken kan utgöra teleövervakning att hindra telemeddelanden från att nå fram.[37]

Detta illustrerar väl behovet av att bereda de generella rättsfrågor som aktualiseras vid en övergång till IT så att de olika regelverkens fungerande inre samband inte bryts upp till följd av de tekniska och administrativa förändringarna.

12.4 Processrättsliga frågor

12.4.1 Bakgrund

Inom Justitiedepartementet övervägs Datastraffrättsutredningens betänkande Information och den nya InformationsTeknologin — straff- och processrättsliga frågor (SOU 1992:110), samt Polisrättsutredningens betänkande Tvångsmedel enligt 27 och 28 kap. RB samt polislagen (SOU 1995:47), där bl.a. bestämmelserna om husrannsakan och beslag tas upp, huvudsakligen från traditionell utgångspunkt.

Även internationellt bedrivs arbete på området. Bl.a. har det nyligen inom Europarådet utarbetats en rekommendation No. R (95) 13 angående straffprocessuella frågor med anknytning till IT.

De bestämmelser jag föreslår i en särskild lag om elektroniska förmedlingstjänster syftar bl.a. till att göra det möjligt att utreda brott. Intresset av effektivitet i den brottsutredande verksamheten måste emellertid vägas mot intresset av skydd för motstående intressen.

Det faller utanför mitt uppdrag att ta ställning till vilka allmänna principer som bör gälla för de brottsutredande organens verksamhet på IT-området. Nya rättsfrågor aktualiseras emellertid till följd av användningen av sådana "elektroniska platser" (eller "kvasimateriella utrymmen" med Datastraffrättsutredningens terminologi) som utgörs av elektroniska förmedlingstjänster.[38]

De okonventionella metoderna för kommunikation via sådana förmedlingstjänster väcker frågor om hur spaning och brottsutredning

[37] Prop. 1994/95:227.

[38] IT-miljön är av sådan karaktär att det finns vissa "elektroniska platser" till vilka en stark misstanke om brottsliga aktiviteter kan knytas, samtidigt som det är vanligt att polisen inte känner till "platsernas" struktur i detalj eller något konkret brott och vem som kan misstänkas för detta. Missbruket består vanligtvis inte i sådan grov brottslighet som kan motivera mer ingripande tvångsmedel. Samtidigt kan effektiv brottsbekämpning knappast ske med traditionella metoder i denna miljö.

skall kunna bedrivas med konventionella metoder. Dessa frågor har emellertid ett direkt samband med de grundläggande och principiella straffprocessuella frågorna på IT-området. Jag begränsar därför mina överväganden till några allmänna synpunkter rörande frågan om åtkomst till uppgifter, m.m.

Bestämmelserna i 27 och 28 kap. rättegångsbalken är tillämpliga också vid förundersökningar rörande elektroniska förmedlingstjänster, och regleringen torde vara att tolka så att verkställighet kan äga rum även med avseende på data.[39] Eftersom brottsliga förfaranden med anknytning till elektroniska förmedlingstjänster äger rum via telekommunikationer framträder emellertid vissa skillnader. Polisen äger inte rätt att "följa efter" en misstänkt "i nätet". Det kan, med hänsyn till risken för otillbörligt integritetsintrång, endast undantagsvis komma i fråga att avlyssna eller övervaka telekommunikationer.[40]

I det följande tar jag upp vissa frågor som aktualiseras när en polisman via modem och telenät avser att, utan användning av tvångsmedel, utforska en viss elektronisk förmedlingstjänst.

12.4.2 Är allmänt tillgängliga förmedlingstjänster tillgängliga för polisen?

När en elektronisk förmedlingstjänst är tillgänglig utan att användarna behöver ange sin identitet kan naturligtvis också en polisman få koppla upp sig; jfr att en polisman läser annonser och klipper ut vissa som är av intresse. Så snart det krävs att användaren anger sin identitet begränsas emellertid förutsättningarna för spaning.

En polisman har i princip samma befogenheter som en privatperson, men inom den öppna polisverksamheten torde det inte godtas att oriktiga identitetsuppgifter lämnas, inte ens om övriga användare använder täcknamn.[41] Vid t.ex. spaning uppträder polisen visserligen i civila kläder och ger sken av att vara privatpersoner, eftersom det är en förutsättning för åtgärden att inte avslöja att den vidtas i tjänsten. Att uppträda civilklädd är emellertid inte helt jämförbart med att under oriktigt namn bereda sig tillträde till en elektronisk förmedlingstjänst.

[39] Jfr dock SOU 1995:47 s. 184 f. I sammanhanget bör Datastraffrättsutredningens förslag nämnas, att som en ny 28 kap. 1 a § RB föra in, dels en utvidgad rätt till husrannsakan, när det kan antas att en elektronisk anslagstavla innehåller data som är ägnade att användas vid brott eller vilkas spridande utgör brott (jfr 28 kap. 3 § RB), dels den begränsningen att husrannsakan i annat fall bör få ske via telenät endast om särskilda skäl föreligger.

[40] Se vidare de förutsättningar som enligt 27 kap. rättegångsbalken gäller för hemlig teleavlyssning och hemlig teleövervakning; jfr Datastraffrättsutredningens förslag i 27 kap. 3 b § andra stycket rättegångsbalken.

[41] Jfr Justitiekanslerns beslut den 26 september 1994 enligt vilket polisen inte ansetts äga rätt att som ett led i den brottsbekämpande verksamheten lämna vilseledande information till massmedia, dnr. 1590-94.

En civilklädd polis ställs vanligtvis inte i en situation där medvetet felaktiga identitetsuppgifter krävs för att fullfölja åtgärden, och det anses, som framgått, att en polisman i den öppna polisverksamheten inte får lämna osanna uppgifter.

En polisman som är okänd i aktuella kretsar bör dock kunna använda sitt rätta namn och få tillgång till en elektronisk förmedlingstjänst. Poliser som är erfarna på området blir emellertid sannolikt stoppade vid uppkopplingen eller hindras från att få tillgång till material som styrker brott. I praktiken bör detta kunna lösas genom att en polis som inte är känd i aktuella kretsar, under ledning av en polis som har erfarenheter av IT-området, kopplar upp sig i eget namn, varefter båda kan ta del av uppgifterna.

När det krävs muntliga kontakter — i vissa fall personliga rekommendationer — för att godkännas som användare, torde en polisman inte kunna bereda sig åtkomst till förmedlingstjänsten utan beslut om husrannsakan. För att bli insläppt, utan användning av tvångsmedel, skulle polismannen bli tvungen att "låna" en användares identitet eller vilseleda om sin identitet vid samtal med den som tillhandahåller tjänsten samt — när det krävs — skaffa rekommendationer från en annan användare. Istället för att få uppgifter från en informatör skulle polismannen härigenom bli infiltratör.

Sådana okonventionella spaningsmetoder kan, i enlighet med de principer som slagits fast i samband med att polislagen antogs, knappast komma i fråga inom den öppna polisverksamheten.[42] Det är som framhållits tidigare betydelsefullt att möjligheterna att utreda brott i IT-miljön förbättras, men man kommer då in på frågor av sådan natur att de bör övervägas i ett större sammanhang.

12.4.3 Brottsliga förfaranden vid spaning och utredning?

En fråga, som är begränsad till elektroniska förmedlingstjänster, rör de s.k. menyer som möter en användare som kopplar upp sig mot en elektronisk förmedlingstjänst. Det förekommer att menyn innehåller ett meddelande om att t.ex. poliser och åklagare inte medges tillträde till förmedlingstjänsten. Ett sådant meddelande medför emellertid inte att poliser och åklagare som kopplar upp sig begår brott. Den som tillhandahåller förmedlingstjänsten kan uppenbarligen inte på detta sätt förfoga över olovlighetsrekvisitet i t.ex. bestämmelsen om dataintrång (21 § DL).

[42] Se vidare prop. 1984/84:111 s. 46 f.; jfr Axberger, Hans-Gunnar, Brottsprovokation, 1989.

En annan fråga som kompliceras av de nya rutinerna har samband med principen att polisen aldrig får provocera till brott eller begå en kriminaliserad handling för att kunna efterforska eller avslöja brott. Denna regel kan komma i konflikt med själva rutinerna för att ta del av innehållet i en elektronisk förmedlingstjänst. Att säkra materialet på en databärare hos polisen kan nämligen resultera i t.ex. en otillåten exemplarframställning enligt upphovsrättslagen. Antingen kan en polisman som genomför åtgärden uppfylla brottsrekvisiten eller också kan t.ex. den som tillhandahåller tjänsten "provoceras" till ett brott.

Vid motsvarande åtgärder i traditionell miljö inriktas åtgärderna mot traditionella fysiska exemplar. Om dessa exemplar är tillgängliga för var och en, kan de läsas och t.ex. fotograferas av polisman utan att han riskerar att begå brott. I IT-miljön kan emellertid en användning av tvångsmedel krävas för att frita från straffansvar.

Det är inte heller i denna del lämpligt att lagreglera s.k. förspaning och spaning inom ramen för en förundersökning. Förhållandena i de enskilda fallen växlar och utvecklingen på IT-området sker snabbt. Polisen bör emellertid från fall till fall noga överväga hur åtgärderna utformas så att resultat som inte är avsedda kan undvikas.

Slutligen vill jag beröra vilka åtgärder som är möjliga när en elektronisk förmedlingstjänst har hemligt telefonnummer och den som tillhandahåller tjänsten endast anger ett täcknamn. Enligt 25 och 27 §§ telelagen (1993:597) får en teleoperatör lämna ut uppgifter om teleabonnemang som angår misstanke om brott, om fängelse är föreskrivet för brottet och detta, enligt myndighetens bedömning, kan föranleda annan påföljd än böter; jfr 14 kap. 2 § sekretesslagen (1980:100).

Innan en konkret misstanke om brott föreligger kan det alltså vara så att de brottsutredande organen inte ens kan få besked om vem som har en viss teleadress och — när anslutningen av abonnenten skett till en viss geografisk punkt — var inkoppling till nätet har skett. Mitt förslag, att vid straffansvar ålägga den som tillhandahåller en elektronisk förmedlingstjänst att underrätta dem som vill ansluta sig om vem som tillhandahåller denna, bör kunna underlätta den brottsutredande verksamheten.

12.5 Konsekvenser av mina förslag

Av problemanalysen ovan (se bl.a. avsnitt 11.3) framgår att åtgärder behöver vidtas, samtidigt som svårigheterna är uppenbara att komma åt brottslig eller annars oacceptabel informationsspridning via elektroniska förmedlingstjänster. Det har till och med visat sig vara svårt att få tillförlitligt underlag för att bedöma problemens omfattning. Det brukar emellertid antas att det finns ca 6 000 elektroniska anslagstavlor i Sverige och att omfattande missbruk förekommer i kanske ett hundratal.

Mer oklart är hur många förmedlingstjänster knutna till Internet som tillhandahålls i Sverige. Gissningsvis kan det finnas kanske 500, men de ökade möjligheterna att — med nya versioner av programvaror för informationsutbyte via Internet — själv lägga upp s.k. hemsidor, för med sig att antalet kan antas komma att öka kraftigt.

Brottslig eller annars oacceptabel spridning av information bör som sagt i första hand mötas genom etiska regler och andra frivilliga åtgärder. Sådana åtgärder får emellertid knappast någon verkan beträffande förmedlingstjänster som bedrivs med inriktning på brottslig informationsspridning. De frivilliga åtgärderna behöver därför stödjas av författningsregleringen.

Visserligen kan den föreslagna regleringen delvis kringgås genom att verksamheter flyttas utom riket. Förslagen har emellertid, som framgått av avsnitt 11.7, utformats med tanke på att sådana åtgärder i viss mån skall kunna mötas, och regleringen kan antas leda till en betydande självsanering. Enligt min mening överväger alltså fördelarna med den föreslagna regleringen, under förutsättning att de kostnader och andra belastningar som läggs på den som driver verksamheten kan hållas på en rimlig nivå.

Det föreslagna osanktionerade stadgandet om uppsikt över tjänsten (3 §) får läsas i ljuset av bestämmelsen om förhindrande av fortsatt spridning (5 §), som blir tillämplig endast när den som tillhandahåller tjänsten eller på hans uppdrag har tillsyn över tjänsten känner till att ett meddelande av den angivna karaktären tillhandahålls via den elektroniska förmedlingstjänsten. Det krävs alltså inte att den som är ansvarig sitter och går igenom alla meddelanden som förmedlas. När han till följd av sin egen tillsyn av tjänsten, en upplysning från en användare eller på något annat sätt får vetskap om att ett meddelande som tillhandahålls är av sådan karaktär att fortsatt spridning skall förhindras bör åtgärden relativt enkelt kunna vidtas. Jag har nämligen inhämtat att en fil med visst namn eller ett visst ord eller uttryck snabbt kan sökas fram med sådana funktioner som vanligtvis ingår i de programvaror som används för elektroniska förmedlingstjänster. Har den ansvarige, efter underrättelse om att visst missbruk skulle förekomma, letat efter materialet utan att kunna finna det föreligger ingen uppsåtlig överträdelse av regleringen.

Det bör alltså, för verksamheter som inte syftar till brottslig spridning av information och som inte direkt blir måltavla för vissa användares missbruk, vara fråga om försumbara kostnader att tillgodose de minimikrav jag har föreslagit för elektroniska förmedlingstjänster. Kostnaderna för dem som strävar efter att vara laglydiga kan till och med minska genom att rättsläget klarläggs. Motsatsen gäller naturligtvis för tjänster som nu delvis är inriktade på t.ex. sådan informationsspridning som är brottslig.

Det är alltså mycket svårt, för att inte säga omöjligt, att i direkta siffror ange vilka kostnader mina förslag kan antas föra med sig. Vad beträffar skyldigheten att underrätta om vem som tillhandahåller tjänsten m.m. (förslaget till 4 §) är det ingen tvekan om att kostnaderna är försumbara. Ett försök till beräkning av kostnaden för att hindra spridning skulle visserligen kunna utformas enligt följande. Om man antar att det finns 6 500 förmedlingstjänster, att det i genomsnitt tar en timma i veckan att vidta åtgärder för att förhindra spridning och att timkostnaden är 500 kr, skulle årskostnaden bli 169 miljoner kr. Siffran bygger emellertid på så grova antaganden att den inte kan anses ge någon vägledning. För sådana tjänster som drivs av det allmänna kan det dock, med hänsyn till bl.a. verksamhetens inriktning, antas att kostnaderna blir i det närmaste försumbara.

Min slutsats är alltså att de skyddsintressen som den förslagna regleringen vilar på får anses väga över de kostnader och olägenheter som förslaget kan föra med sig.

Särskilda yttranden

Av experten *Göran Axelsson*

IT-utredningen gör ett banbrytande arbete i svensk förvaltning vad gäller att söka lägga en rättslig grund för att ge myndigheter, allmänhet och organisationer möjlighet att på ett betryggande sätt överföra elektroniska handlingar. Dessa handlingar ska inte behöva åtföljas av brev, fax eller förklarande telefonsamtal.

IT-utredningen har lagt ned betydande tid på att söka klarlägga de grundläggande begrepp som lagarna bör utgå ifrån. Utredarens förslag till terminologi återfinns i "Förslag till lag om ändring i förvaltningslagen (1986:223)". Där definieras

— elektronisk handling
— digitalt dokument
— digital signatur
— digital stämpel.

Jag anser att "digital signatur" kan härröra från såväl en fysisk person som en organisation. Det torde vara i överensstämmelse med de lösningar på samma problem som finns eller kommer fram i andra länder och i Europeiska unionen.

Begreppet "digital stämpel" behövs inte i lagstiftningen. IT-utredningen knyter samma regelverk till båda begreppen. Det skapar förvirring för organisationer och allmänhet att i lagar och förordningar ha med det extra begreppet "digital stämpel". Problemen i samhället att gå över från pappershandlingar till elektroniska handlingar är komplicerade. Det behövs ett stort mått av pedagogik från samhällets sida för att ge människor och organisationer vägledning.

Tanken om "digital signatur" jämförd med "digital stämpel" kommer från visionen om att *en* person ska ha *en* digital signatur och att *en* organisation ska ha *en* digital stämpel.

I praktiken kommer mottagare av digitala dokument att behöva verifiera avsändaren genom att kontrollera dennes identitet, t.ex. i en elektronisk databas (s.k. CA-funktion). Människor och organisationer har många skilda roller och är behöriga att göra många olika handlingar. Jag bedömer det som orealistiskt — och dessutom som ytterst olämpligt — att införa *en* databaslösning i Sverige där alla människor och organisationer är registrerade med sina unika signaturer respektive

stämplar och med uppgifter om vilka behörigheter som är giltiga för stunden.

Det rimliga är i stället att arbetsgivare delar ut digitala signaturer till egna anställda som behöver sådana, samt upprättar en egen elektronisk förteckning över dem som är behöriga. Denna förteckning kan sedan länkas till andra förteckningar. Arbetsgivaren, dvs. organisationen, väljer också vilka digitala signaturer som den behöver. Kanske ska det elektroniska blankettförrådet ha en egen digital signatur. Banker och andra tjänsteleverantörer får utarbeta lösningar för sina kunder (företag och allmänhet). Stat, kommun och landsting får utarbeta lösningar för elektronisk kommunikation med medborgare och organisationer.

Kanske finns det utrymme på marknaden för en eller flera CA-funktioner — som är gemensamma för många tjänster — om kunder och tjänsteleverantörer önskar detta.

Svårigheterna i IT-utredningen att komma fram till en gemensam uppfattning om terminologin bottnar i att vi inte säkert vet hur system för elektroniska handlingar och digitala signaturer med rättsverkan bör fungera, eller kommer att fungera i praktiken.

Terminologin är grundläggande och bör inte bli felaktig. Det kommer många att ångra under kommande decennier. Regeringen bör först söka klarlägga hur dessa nya system bör vara utformade, innan någon lagändring genomförs.

Om man nu ändå vill genomföra förändringarna — det finns många skäl för detta — är det enklast att bygga på begreppen "elektronisk handling", "digitalt dokument" och "digital signatur" (både personer och organisationer kan ha sådana). Då har vi i Sverige goda möjligheter att göra oss förstådda utomlands. Om det senare, när ökad klarhet vunnits om hur verkligheten ter sig, visar sig att begreppet "digital stämpel" behövs i lagstiftningen kan detta begreppet införas av regering och riksdag.

Av experten *Ingela Halvorsen*

I betänkandet föreslår utredaren en ny lag om tjänster för förmedling av elektroniska meddelanden.

Elektroniska meddelanden utväxlas i en ökande omfattning. Inte minst gäller detta för den typ av kommunikation där mottagarna av ett meddelande är en obestämd och för avsändaren okänd grupp av individer, dvs. den typen av informationsutbyte som vanligtvis sker via öppna nät t.ex. Internet. Denna typ av kommunikation är till helt övervägande del av oskyldigt slag och motiverar inte någon särskild reglering från statsmakternas sida.

Det finns emellertid utan tvekan problem förknippade med ett fritt informationsflöde via öppna nät. Från de utgångspunkter som aktualiseras av utredningsuppdraget kan det konstateras, att dessa problem så gott som alltid avser spridande av barnpornografi, rasistiska uttalanden eller andra förkastliga meddelanden, t.ex. uppmaningar att begå brott eller anvisningar om tillvägagångssätt för att begå brott. S.k. piratkopiering av upphovsrättsligt skyddade verk brukar också nämnas i dessa sammanhang. Vid ett närmare skärskådande torde det visa sig att så gott som samtliga oacceptabla beteenden redan är kriminaliserade i dag. Det som inte kan accepteras från samhällets sida är att det i den elektroniska världen är så svårt eller ibland omöjligt att finna och identifiera en gärningsman. En eventuell reglering bär därför i första hand ta sikte på att lösa detta problem.

Från datalagsrättsliga utgångspunkter utgör denna form av åsiktsutbyte eller kommunikation, som förekommer i öppna nät, inte några nämnvärda problem. De få personregister som finns, t.ex. register över användare, är från integritetsskyddssynpunkt av harmlöst slag. Den omständigheten som nämns i direktiven till utredaren, nämligen att Datainspektionen beviljat få tillstånd för elektroniska anslagstavlor, torde hänga samman med att de flesta sådana är register som kan inrättas och föras endast med stöd av licens och utan krav på tillstånd enligt datalagen. En licens torde de flesta seriösa informationsspridare ha redan i dag. Förekomsten av elektroniska anslagstavlor kommer således inte särskilt till uttryck i inspektionens diarium eller statistik. Några särskilda problem i de avseenden som nu är i fråga har inte heller uppmärksammats i Datainspektionens tillsynsverksamhet.

Den föreslagna lagens tillämpningsområde är inte avgränsat på ett sådant sätt att det blir lätt för den enskilde att förstå, om han omfattas av lagstiftningen eller inte. Faran är att den alltmer tilltagande digitaliseringen av olika traditionella tekniker på sikt leder till att tillämpningsområdet kommer att omfatta snart sagt all informationshantering, i den mån inte någon av undantagssituationerna i lagens

inledningsstadgande är tillämplig. Regleringen riskerar då att bli en reglering av en viss teknik. Jag ställer mig därför tveksam till om den föreslagna lagstiftningen kan nå sitt syfte.

Kommittédirektiv

Rättsliga överväganden kring informationsteknologi

Dir. 1994:42

Beslut vid regeringssammanträde 1994-05-19

Sammanfattning av uppdraget

En särskild utredare tillkallas med uppgift att utarbeta sådana förslag till rättslig reglering som kan behövas i samband med inrättandet av s.k. elektroniska anslagstavlor och för användningen av elektroniska dokument inom både förvaltningen och näringslivet.

Har tekniken sprungit ifrån lagstiftningen?

I den senaste finansplanen (prop. 1993/94:100 bil. 1) pekade regeringen ut informationsteknologi som ett område för infrastrukturella investeringar. Regeringen anförde också bl.a. att informationssamhällets elektroniska infrastruktur inte bara omfattar en fysisk nätuppbyggnad. Det handlar också om en anpassning av lagstiftning och övriga regler till den moderna informations- och kommunikationstekniken (prop. s. 62).

Datalagen (1973:289) syftar till att skydda den enskilde mot otillbörligt intrång i den personliga integriteten till följd av att personuppgifter registreras med hjälp av automatisk databehandling (ADB). Datainspektionen har till uppgift att pröva ansökningar om tillstånd och utöva tillsyn enligt denna lag.

Lagen kom till år 1973 och var den första lagen i världen av denna typ med nationell räckvidd. Redan vid dess tillkomst

2

förutsattes att lagen skulle ses över inom en snar framtid. Så har också skett i olika etapper. Den senaste utredningen på området, Datalagsutredningen, lade fram sitt slutbetänkande En ny datalag (SOU 1993:10) i februari 1993. I den på betänkandet grundade prop. 1993/94:116 Normgivningsfrågor på dataskyddsområdet, m.m. har regeringen i samband med förslag till grundlagsändringar på dataskyddsområdet förklarat att frågan om att stifta en ny datalag bör anstå till dess att det finns ett slutligt ställningstagande av EU:s medlemsländer till det förslag till dataskyddsdirektiv EG-kommissionen lade fram i oktober 1992. Däremot menade regeringen att detta inte hindrade genomförandet av angelägna ändringar i det nuvarande systemet. I prop. 1993/94:217 En reformerad datalag har regeringen lagt fram de förslag till ändringar som aviserades i grundlagspropositionen.

Vid sidan av de ändringar som behandlas i prop. 1993/94:217 kan det emellertid konstateras att den snabba tekniska utvecklingen reser ytterligare frågor om tillämpningen av datalagen. Det är särskilt i några konkreta situationer som förhållandet mellan nuvarande datalagstiftning och kommunikationen med hjälp av modern informationsteknologi har aktualiserats.

Elektroniska anslagstavlor

Den tekniska utvecklingen av datorer och av lagringsmöjligheter samt åtkomst av datafiler innebär ökade möjligheter att på ett enkelt och billigt sätt kunna sprida information med hjälp av datorer. Ett led i denna utveckling har blivit upprättandet av databaser med möjlighet för stora grupper av användare att tillföra databasen egna meddelanden och läsa andras insända meddelanden, s.k. elektroniska anslagstavlor (Bulletin Board Systems - BBS). Enskilda som uteslutande för personligt bruk inrättar och för elektroniska anslagstavlor torde inte omfattas av datalagens regler om licens- och tillståndsplikt. En näringsidkare eller en myndighet som vill inrätta en sådan elektronisk anslagstavla med möjlighet att be-

3

arbeta personuppgifter ställs emellertid inför frågan om detta också innebär att ett personregister i datalagens mening inrättas. Uppgifter som i datalagens mening är känsliga, t.ex. politisk åskådning, värderingar och omdömen kan komma att registreras. Sådana register kräver i princip tillstånd av Datainspektionen. Enligt uppgift från Datainspektionen finns bara ett sådant tillstånd och det meddelades före år 1982, dvs. under en period då i princip alla personregister var tillståndspliktiga. Samtidigt är det bekant att ett stort antal elektroniska anslagstavlor har inrättats. Sannolikt borde flera av dessa prövas enligt datalagens regler.

En bestämmelse som i detta sammanhang tycks föranleda tillämpningssvårigheter är att datalagen (och sekretesslagen för myndigheter), om inte Datainspektionen först gett sitt medgivande, förbjuder utlämnande av en personuppgift ur personregister om uppgiften kan antas bli använd för automatisk databehandling i utlandet och det inte rör sig om ett land som anslutit sig till Europarådets dataskyddskonvention. Inte ens alla EU-stater är anslutna till konventionen. Detta innebär att en näringsidkare eller en myndighet som inrättar en elektronisk anslagstavla och därvid till t.ex. USA sprider information som innehåller personuppgifter kan komma att bryta mot datalagen respektive sekretesslagen.

Ytterligare en komplikation vid inrättandet av elektroniska anslagstavlor kan datalagens regler om registeransvar vara. Den registeransvarige ansvarar för riktigheten av personuppgifter som förekommer i ett register, bl.a. genom ett strikt skadeståndsansvar. Den registeransvarige skall också rätta oriktiga och missvisande uppgifter i sitt register. Att kontrollera den strida ström av meddelanden som kan förekomma i en elektronisk anslagstavla kan bli svårt. Registeransvaret i sig tycks alltså förutsätta någon form av förhandskontroll av de uppgifter som förs in i en elektronisk anslagstavla. En sådan förhandsgranskning är knappast möjlig att förena med syftet med den form av öppet forum för åsiktsutbyte som en elektronisk anslagstavla ofta skall utgöra. Som Datastraffrättsutredningen framhållit i sitt betänkande Information och den nya

4

InformationsTeknologin (SOU 1992:110, s. 364 ff.) har vissa elektroniska anslagstavlor visat sig utgöra forum för informationsutbyte om förfaringssätt vid brott, otillåten programkopiering etc. Straffrättsliga aspekter aktualiseras således också i sammanhanget.

Den yttrandefrihetsrättsliga lagstiftningen kan också aktualiseras. Yttrandefrihetsgrundlagens (YGL) föreskrifter om radioprogram tillämpas enligt 1 kap. 9 § YGL också på mediaföretag som tillhandahåller allmänheten upplysningar direkt ur ett register med upptagningar för ADB. Som ett exempel kan nämnas att i en riksdagsmotion (1993/94:K208) har frågor om ansvarigt utgivarskap för elektroniska anslagstavlor tagits upp. Datastraffrättsutredningen för sin del fann det snarast som orealistiskt med bestämmelser motsvarande ansvarigt utgivarskap (a.a. s. 366). Diskrimineringsombudsmannen har i en skrivelse till regeringen tagit upp frågor om spridande av främlingsfientliga budskap i elektroniska anslagstavlor.

Enligt tryckfrihetsförordningens (TF) regler om allmänna handlingar är en ADB-upptagning att anse som förvarad hos myndigheten om myndigheten faktiskt disponerar över möjligheten att föra över upptagningen till läsbar eller annan uppfattbar form. Om en upptagning utgör ett personregister (med personregister förstås register, förteckning eller andra anteckningar som innehåller uppgift som avser enskild person och som kan hänföras till denne), krävs därutöver att myndigheten har rättslig befogenhet att föra över upptagningen till läsbar form för att den skall anses som förvarad hos myndigheten. Sådan rättslig befogenhet har myndigheten alltid om inte riksdagen, regeringen eller Datainspektionen har meddelat särskilda begränsningar om vilka uppgifter som får göras tillgängliga.

Enligt sekretesslagens (1980:100) regler måste alla allmänna handlingar antingen diarieföras eller hållas ordnade på annat sätt (15 kap. 1 § sekretesslagen) om inte handlingarna uppenbart är av ringa betydelse för myndighetens verksamhet. Ett undantag från denna regel är då en ADB-upptagning är tillgänglig för flera myndigheter. Under sådana förhållanden

5

behöver endast en av myndigheterna registrera upptagningen (15 kap. 13 § sekretesslagen).

Enligt tidningsuppgifter har världens största kommunikationsnät för datorer, Internet, över 30 miljoner användare. I Internet pågår ett stort antal datakonferenser där olika användare diskuterar med varandra. Om en myndighet aktivt deltar i en elektronisk anslagstavla kan information som är tillgänglig i den bli allmän handling, såvida inte undantagen i 2 kap. 11 § 3 TF (den s.k. biblioteksregeln) blir tillämpliga. Offentlighetsprincipen medför alltså i en sådan situation, försiktigt uttryckt, att ett mycket stort antal uppgifter i ett datorkommunikationsnät som en myndighet deltar i kan bli allmänna handlingar med åtföljande principiell registreringsskyldighet och skyldighet att lämna ut uppgifter.

I sammanhanget bör bestämmelserna i arkivlagen (1990:782) uppmärksammas. I denna ges grundläggande föreskrifter om arkiv hos såväl statliga som kommunala myndigheter samt bestämmelser om bl.a. vad som ingår i en myndighets arkiv samt vård och gallring av arkiv. De bestämmelser som gäller för statliga arkiv gäller också för arkiv hos kyrkokommunala myndigheter, vissa organ som jämställs med myndigheter och allmänna försäkringskassor. Enskildas arkiv regleras dock inte av lagen. Datalagsutredningen behandlade under sitt arbete olika arkivfrågor, främst gallringsfrågor. Utredningen föreslog i sitt slutbetänkande En ny datalag (SOU 1993:10) att det i den föreslagna nya datalagen skulle tas in en allmän bestämmelse om gallring. Närmare regler om gallring på olika områden borde enligt utredningen tas in i särskilda registerlagar eller läggas fast genom rättspraxis.

Elektroniska dokument

Denna utveckling som ökar möjligheterna till informationsutbyte med hjälp av datorer, innebär också en möjlighet att kommunicera med myndigheter och företag genom datorer. Elektronisk post är ett exempel på detta. I sammanhanget uppstår frågor om det kan finnas några särskilda rättsliga

6

problem när ett dokument ges in till en myndighet på endast elektronisk väg. Den tekniska utvecklingen har kommit dithän att möjligheter finns att elektroniskt signera dokument, s.k. digitala signaturer. Denna teknik gör det möjligt att kontrollera att ett dokument inte förändrats och att säkerställa avsändarens identitet.

Förvaltningslagen (1986:223) som reglerar myndigheters handläggning av ärenden, har en reglering som innebär att ett meddelande som kommit in till en myndighet skall bekräftas av avsändaren med en egenhändigt undertecknad handling om myndigheten begär det (10 §). Rättegångsbalken innehåller flera regler om att handlingar måste vara egenhändigt undertecknade. Det gäller bl.a. stämningsansökningar och överklaganden. I prop. 1993/94:190 (bet. 1993/94:JuU30) om enhetliga regler för överklagande till hovrätt och Högsta domstolen m.m. föreslår regeringen att överklaganden och vissa andra skrivelser under en rättegång inte längre skall behöva vara egenhändigt undertecknade. I fråga om stämningsansökningar behålls i förslaget de nuvarande reglerna. Om det behövs får domstolen begära att ett telefax eller annat meddelande som saknar avsändarens underskrift i original bekräftas av avsändaren genom en i original undertecknad handling.

Ett område där utvecklingen som rör kommunikation via ADB kan sägas ha gått längre är tullagens (1987:1065) regler om elektroniska dokument. I 11 a § tullagen har begreppet elektroniskt dokument förts in. Ett elektroniskt dokument sägs där vara en upptagning vars innehåll och utställare kan verifieras genom ett visst tekniskt förfarande. Eftersom förvaltningslagens regler om när en handling skall anses inkommen inte är utformade så att de täcker in elektroniska meddelanden regleras i 12 b § tullagen frågan om när ett elektroniskt dokument skall anses ha kommit in till mottagarmyndigheten. TF:s regler har därvid utgjort en förebild (prop. 1989/90:40 s. 28 ff.). De näringsidkare som Generaltullstyrelsen godkänner ges i detta system för datoriserat uppgiftslämnande rätt att upprätta elektroniska tulldokument och sända in dem via telenätet.

7

Saken har också berörts av Datastraffrättsutredningen i betänkandet Information och den nya InformationsTeknologin (SOU 1992:110).

I regeringens prop. 1993/94:197 Datapantbrev föreslås en reform på fastighetspanträttens område som innebär att pantbrev inte skall behöva utfärdas i skriftlig form. Utöver skriftliga pantbrev av det slag som förekommer i dag skall Centralnämnden för fastighetsdata också kunna utfärda datapantbrev. Framställningar om registrering och avregistrering i pantbrevsregistret skall i stor utsträckning kunna göras med hjälp av ADB. En förebild för propositionens förslag om elektronisk ingivning av ansökningar till pantbrevsregistret är det system med elektroniska dokument som finns i tullagen.

Ansökningar om betalningsföreläggande och handräckning kan göras på medium för automatisk databehandling om så medges av Riksskatteverket enligt 6 och 7 §§ förordningen (1991:1339) om betalningsföreläggande och handräckning. Sådana tillstånd får ges till den som kan antas komma att på ett betryggande och tekniskt ändamålsenligt sätt ge in ett stort antal ansökningar.

Konstitutionsutskottet har i betänkande 1989/90:KU2 (jfr bet. 1990/91:KU11) uttalat att frågan om en reglering av elektroniska dokument i förvaltningsförfarandet måste få en generell lösning. I prop. 1990/91:60 uppmärksammades denna fråga och det uttalades att den föll inom ramen för översynen av datalagen. Som framgått genomförs nu inte Datalagsutredningens förslag till en ny datalag. Utredningen har heller inte närmare berört frågor om rättslig reglering av elektroniska dokument. Lagutskottet har vid behandlingen av prop. 1993/94:197 om datapantbrev framhållit att den reglering beträffande elektroniska dokument som ges i förslaget till lag om pantbrevsregister kan godtas i avvaktan på resultatet av de överväganden om en mer generell reglering av elektroniska dokument i förvaltningsförfarandet som kommer att ske (bet. 1993/94:LU33).

Datastraffrättsutredningen har i sitt tidigare nämnda betänkade behandlat hur en straffrättslig reglering av elek-

8

troniska dokument och digitala signaturer skall kunna ges motsvarande utformning som vad som gäller för brott mot urkunder. Utredningen övervägde också en enhetlig definition av begreppet "handling" för rättegångsbalken efter förebild från tryckfrihetsförordningen (se betänkandet s. 459 ff.). Utredningen berörde vidare frågor om digitala signaturer i rättegångsbalken men lämnade inte något förslag till reglering. Datastraffrättsutredningen menade att en sådan reglering kunde införas först sedan standardiseringen, tillgången till teknisk utrustning osv., nått betydligt längre. Till detta kom att utredningen fann att ytterligare överväganden krävdes.

Tekniken för digitala signaturer är i dag väl utvecklad och det är svårt att förfalska en digital signatur. Inom ramen för Infosec (EC Program for Security of Information Systems) finns standardisering av detta med som ett av fyra utpekade områden. I Sverige har Statskontoret definierat en säkerhetslösning för persondatoranvändning som avses bli en standard, den s.k. Allterminalen. I denna lösning ingår även möjligheten att införa digitala signaturer. Allterminalen håller nu på att införas hos Rikspolisstyrelsen.

Inom den internationella avtalsrättens område analyseras behovet av särskilda regler för användning av EDI (Electronic Data Interchange) vid handel. I detta arbete, som bedrivs av en arbetsgrupp inom Uncitral (United Nations Commission on International Trade Law) diskuteras bl.a. regler om formkrav för elektroniska meddelanden samt regler om utväxling av sådana meddelanden.

Det finns även en informell europeisk grupp av nationella råd benämnd TeleTrusT. Denna organisation syftar till att skapa en öppen säkerhetsstruktur inom informationsteknologiområdet, som kan bli världsstandard. I Sverige representeras organisationen av 18 medlemmar, företrädesvis större svenska företag.

Informationsteknologi i digital form reser vidare en rad frågor om det upphovsrättsliga skyddet för det material som förmedlas med hjälp av en sådan teknologi. Dessa frågor undersöks för närvarande i ett antal andra länder, bl.a. USA

och Japan. Inom Europeiska gemenskapen pågår ett arbete på ett direktiv om det rättsliga skyddet för databaser vilket är av stor betydelse för den internationella informationsförmedlingen, inte bara i Europa utan också mer globalt. Inom Justitiedepartementet pågår en kartläggning av frågorna om informationsteknologins inverkan på det upphovsrättsliga regelsystemet inbegripet dess användning för olika typer av informationssystem (jfr bet. 1993/94:LU16, s. 26).

Informationsteknologikommissionen

Regeringen tillkallade den 17 mars 1994 en kommission för att främja en bred användning av informationsteknologin. Målet för kommissionens arbete anges i prop. 1993/94:177 vara att Sverige senast år 2010 skall "tillhöra den globala utvecklingens absoluta spjutspetsar när det gäller varje del av utnyttjandet av informationsteknologin". En viktig del av kommissionens arbete avses handla om lagstiftningsfrågor.

I samråd med Informationsteknologikommissionen bereds för närvarande inom Justitiedepartementet frågor som bl.a. rör möjligheten att snabbt hitta författningsmässiga lösningar för hur elektroniska anslagstavlor bör hanteras när de inte används uteslutande för enskilt bruk. Detta arbete avses ligga till grund för en försöksverksamhet rörande elektroniska anslagstavlor. På sikt bör dock sökas former för en mer permanent lösning.

Utredarens uppgifter

De tidigare beskrivna exemplen inom olika rättsområden visar på ett i och för sig omfattande behov av analyser av vilka konsekvenser den nya informationsteknologin kan få på olika regelverk. Vad som nu i första hand är aktuellt är emellertid att ta ställning till frågor av mer begränsad karaktär.

10

En analys av konkreta rättsliga frågor som de rörande elektroniska anslagstavlor och frågor om rättslig reglering kring elektroniska dokument och digitala signaturer ligger också väl i linje med det arbete som Informationsteknologikommissionen initierar. Bl.a. förhållandet till datalagen förutsätter i detta sammanhang nya överväganden med beaktande av angelägna integritetsintressen men också med hänsynstagande till behovet av en öppen och fri kommunikation med hjälp av datorer. Även frågor som rör offentlighetsprincipen och den därtill kopplade registreringsskyldigheten i sekretesslagen bör i detta sammanhang analyseras. Likaså torde arkivrättsliga frågor kunna uppstå kring t.ex. hanteringen av elektroniska dokument.

En särskild utredare tillkallas därför för att närmare ta ställning till vissa rättsliga frågor kring informationsteknologin. Utredarens arbete skall vara begränsat till att med beaktande av integritetsintressena lösa de rättsliga problemen kring nämnda frågor om elektroniska anslagstavlor och elektroniska dokument. Vad gäller elektroniska dokument och digitala signaturer kan en fråga vara om några särskilda överväganden behöver göras med hänsyn till reglerna om allmänna handlingars offentlighet och förvaltningsförfarandet eller om det är möjligt att hitta rättsliga lösningar som också innefattar näringslivets behov av reglering av elektroniska dokument.

Det förhållandet att internationellt arbete kan pågå i olika frågor, t.ex. angående digitala signaturer, skall inte hindra utredaren från att analysera och överväga behovet av nationella rättsliga lösningar. I detta sammanhang är det naturligtvis av vikt att utredaren håller sig underrättad om den utveckling som sker i internationella fora och som kan beröra utredningsarbetet.

Frågan om en helt ny datalagstiftning får som regeringen anfört i prop. 1993/94:116 för närvarande anstå till dess klarhet nåtts i frågan om vilket ställningstagande EU tar på integritetsskyddsområdet. Det finns dock anledning för utredaren att i sitt arbete beakta det fortlöpande arbetet inom Europarådet och EU avseende integritetsskyddet för person-

11

uppgifter. Utredaren bör också hålla sig informerad om det utredningsarbete som bedrivs inom Finansdepartementet för att utreda säkerhetsfrågor m.m. vid hantering av s.k. elektroniska akter i skatteregistret.

Utöver det uppdrag som utredaren har att fullfölja kommer det framöver att finnas ett behov av att analysera andra rättsliga frågor som hänger samman med informationsteknologins utveckling och som kan komma att aktualiseras i det arbete som pågår inom regeringskansliet.

Utredningsarbetet skall vara avslutat senast den 1 november 1995.

(Justitiedepartementet)

REGERINGSKANSLIETS
OFFSETCENTRAL
Stockholm 1994

Informationssäkerhet

1 Allmänt

Datoriseringen inom förvaltning och näringsliv har fört med sig ett beroende av IT och sårbara strukturer. Visserligen är frågor om informationssäkerhet relevanta också i traditionell miljö men för den pappersbaserade uppgiftshanteringen finns vedertagna rutiner och tjänster som tillgodoser behovet av skydd. Allmänt sett finns det dessutom mer tid till förfogande vid traditionell hantering av uppgifter. När IT-rutiner skall införas, med bibehållen säkerhet, krävs en ingående analys av såväl tekniska som rättsliga frågor. Säkra rutiner kan vidare vara svåra att förena med högt ställda krav på rationaliseringar och besparingar. Om man bortser från kraven på informations- och rättssäkerhet, kan naturligtvis enskilda åtgärder och transaktioner genomföras snabbare och billigare. När säkerhetsnivån är för låg, är emellertid risken stor för att det uppkommer förluster som tar ut sådana "besparingar".

2 Fysiska resp. logiska skydd

Inom ramen för pappersbaserade rutiner ges tydliga gränser mellan olika handlingar, ärenden, akter, etc. och förvaringen av en handling hos en viss myndighet eller ett visst företag kan enkelt skiljas från en förvaring på annan plats. Dessa gränser, som uppfattas som självklara, ligger till grund för författningsregleringen.

I IT-miljön framträder en mer komplicerad bild. De traditionella gränserna ersätts av ett slags "gränslöshet" där olika medier och tillämpningar flyter samman. Uppgifter kan sekundsnabbt bearbetas och överföras långa sträckor, samt finnas tillgängliga för flera användare samtidigt via terminaler eller genom att lagras samtidigt i flera informationssystem. Denna "gränslöshet" är inte en slump utan en medveten strävan efter effektiva och generella rutiner för informationsbehandling.

De hot som framträder i IT-miljön har stegvis mötts av elektroniska motsvarigheter till det traditionella skyddet för information. *Ett fysiskt skydd*, t.ex. att låsa in all teknisk utrustning i säkra utrymmen, kan dock endast i speciella fall lösa problemen eftersom de nya rutinerna ofta bygger på möjligheten att sekundsnabbt transportera data via allmänt tillgängliga telenät och att behandla känsliga data i informationssystem som i princip är öppna för vem som helst. Därför har *logiska skydd* utvecklats, baserade på bl.a. lösenord och kryptering. Fysiska skydd kan emellertid även i framtiden antas komma att fylla viktiga funktioner, bl.a. i anknytning till moderna metoder för att signera elektroniska

handlingar. Som exempel kan nämnas sådana kreditkortsliknande s.k. aktiva kort och andra moduler för informationssäkerhet, som avses förhindra åtkomst till hemliga nycklar och annan information som annars skulle kunna missbrukas.

3 Digitala signaturer som säkerhetsfunktioner

3.1 Traditionella underskrifter

En underskrift med bläck ger ett verksamt skydd mot manipulationer. Underskriften låses vid pappersarket med dess text, eventuellt i förening med stämplar, vidimering eller andra äkthetstecken. I vissa fall följer krav på sådana rutiner direkt av författningsregleringen, i andra sammanhang har mellanhavandet den karaktären att det framstår som självklart att i skrift bekräfta vad som gäller.

De funktioner en underskrift därvid fyller uppfattas vanligtvis som självklara. Underskriften *identifierar* den som har undertecknat samtidigt som den har den ovan beskrivna *äkthetsfunktionen*, dvs. att ge tillit till att viss text omanipulerat härrör från den som framstår som utställare. Underskriften fyller också en *bevisfunktion*, tillsammans med uppgifterna i den undertecknade handlingen. Den som undertecknat, knyts vanligtvis på ett säkert sätt till innehållet, och underskriften ger uttryck för en vilja att bekräfta och binda sig vid den undertecknade texten. Underskriften har vidare en *avslutsfunktion* och en *varningsfunktion*. Den som undertecknar ger uttryck för att den text som underskriften avser har fått sin slutliga utformning och den som skall skriva sitt namn blir medveten om att åtgärden kan medföra rättsliga förpliktelser.[1]

3.2 Den digitala signaturen

Digitala signaturer skiljer sig i väsentliga avseenden från traditionella namnteckningar. Den grundläggande principen för framställning av en digital signatur är att data, som representerar t.ex. en handling som skall signeras, databehandlas med en krypteringsalgoritm (en matematisk beräkningsregel) i förening med en personlig nyckel, unik för den individ som skall utföra signeringen. Resultatet av denna beräkning blir ett kontrolltal, som är "unikt" för denna händelse, och som vanligtvis kan kontrolleras av någon annan, utan att signatärens personliga nyckel behöver röjas eller annars göras tillgänglig så att den riskerar att komma till obehörigas kännedom.

[1] Lindberg, Elektroniska originaldokument och elektronisk signatur, s. 30 f. och Hiselius, Elektroniska avtalsslut med signatur, s. 64 f.; IRI-rapport 1987:7 och 1989:2.

Den digitala signaturen består alltså inte av undertecknarens namn utan av en serie "meningslösa" siffror som är en unik funktion av både datainnehåll och signatärens identitet.[2] Knytningen av signaturen till individen sker genom en för varje person eller organisation unik kryptonyckel, som skall hemlighållas, till skillnad från traditionella underskrifter, som skyddas mot missbruk genom att de är fysiskt knutna till en enda individ genom dennes unika sätt att skriva sitt namn.[3] I praktiken krävs datorkapacitet för att kunna verifiera den digitala signaturen, även om den i och för sig också kan skrivas ut på papper.

Experterna på IT-området synes vara eniga om att teknik för signering, baserad på rutiner för kryptering, gör det möjligt att lösa många av de frågor om gränser och säkerhet som framträder i IT-miljön. Sådana rutiner kan tillämpas på all digitaliserad information, oberoende av om den representerar text, bild, ljud eller kombinationer därav.[4]

En fråga som bör nämnas i sammanhanget är dock hur användaren skall kunna veta vad han signerar. Vid användning av pappershandlingar är det bara att läsa innantill före undertecknandet, medan den som signerar digitalt behöver kunna lita på det tekniska system i vilket informationen presenteras, inte bara på sitt eventuella personliga signaturverktyg, t.ex. ett aktivt kort.

3.3 Nyckelhanteringen och tilliten till signaturer

En avgörande fråga för tilltron till en digital signatur är hur man kan säkerställa att den individanknutna hemliga informationen som används vid signering endast kan brukas av dess rätte innehavare. Området kallas allmänt "nyckelhantering" efter engelskans "Key Management".

[2] Enligt svensk standard definieras *digital signatur* som omvandling av ett meddelande (eller ett kondensat av detta) på ett sätt som endast avsändaren kan utföra och som tillåter mottagaren att kontrollera meddelandets äkthet, innehåll och avsändarens identitet. Internationella standardiseringskommissionen har definierat "digital signature" enligt följande: "Data appended to, or a cryptographic transformation of, a data unit that allows the recipient of that data to prove the source and integrity of the data unit. It protects against forgery, even by the recipient" (ISO 7498-2). Dessa rutiner beskrivs i bl.a. SOU 1989:20 s. 69 f. och SOU 1992:110, bl.a. s. 252 f. och 275 f. och Ds 1994:80 s. 79 f. Metoden att bereda skydd genom att en terminalanvändare måste bekräfta sin identitet genom ett hemligt *lösenord* kan visserligen rätt utformad binda en utställare till ett dokument lagrat inom ett specifikt fysiskt system med någon form av skydd, men en sådan metod låser inte textens innehåll så att man kan veta att den inte är förvanskad.

[3] En underskrift som görs med teknisk utrustning så att den framträder på bildskärm när den "undertecknade" texten läses är inte verkningsfull. Den som har tillgång till en sådan handling kan enkelt kopiera data som representerar underskriften och med stöd av IT knyta den underskriften till någon annan text; jfr fotokopior och telefaxmeddelanden som enkelt kan manipuleras.

[4] Därmed kan gränserna mellan vad som bör ses som skriftlig resp. muntlig kommunikation komma att delvis suddas ut.

Nycklar för kryptering måste skyddas mot missbruk såväl av utomstående som av nyckelinnehavaren. Härvid avses i första hand nycklar för signering och autenticering, men även nycklar för sekretesskydd. Den metod de flesta säkerhetsexperter idag rekommenderar innebär en användning av s.k. aktiva kort, som skall bäras som personliga "värdehandlingar".[5] I sådana kort och annan liknande utrustning kan de kryptografiska beräkningarna göras utan att den personliga nyckeln överhuvud taget blir exponerad. Om ett sådant verktyg för signering skulle komma på avvägar, ges ändå ett skydd genom att ett lösenord eller en personlig kod, vanligtvis bestående av 4-5 siffror, måste anges till kortet varje gång det skall användas.[6]

Dessa funktioner kan ge en lika effektiv kontroll av en handlings äkthet som en namnteckning på ett papper. Det digitala dokumentets äkthet kontrolleras automatiskt beträffande både innehåll och utställare, och kontrollen blir från teknisk synpunkt i princip felfri.

Olika tekniska metoder har utvecklats och det pågår ett intensivt internationellt arbete när det gäller hur frågor om verifiering skall lösas för att säker kommunikation skall bli möjlig alla-till-alla. Ett viktigt tekniskt bidrag är utvecklingen av kryptografiska metoder för signaturer där en annan nyckel används för verifiering av en signatur än den privata nyckel som har använts för att skapa denna (s.k. asymmetriska kryptosystem). En sådan s.k. publik nyckel kan öppet distribueras till alla som behöver kunna verifiera en viss individs signatur.

Åtminstone i vissa sammanhang torde det behövas en betrodd part, som utan att ha egna intressen i den information som förmedlas, har uppgiften att registrera användare, utfärda och administrera nycklar för kryptografiska signaturer och annars fullgöra de funktioner som behövs för användningen av digitala dokument och anknytande rutiner för informationssäkerhet.[7]

Som nyss angetts blir en kontroll av detta slag från teknisk synpunkt i princip felfri. Det är i stället kontrollen av vem som har utnyttjat en bestämd nyckel som utgör rutinens svaghet. Den som har fått tag på ett kort för signering och koden till kortet kan framställa digitala signaturer

[5] Det kan i vissa sammanhang vara önskvärt att rutinerna utformas så att en signatur inte bara härrör från en viss nyckel som en gång delats ut till en individ, utan också så att signeringen måste ske med ett aktivt kort (eller en annan unik säkerhetsmodul). Dels ger det bättre möjligheter att binda innehavaren till handlingen, dels kan en nyckel som missbrukas återtas genom att kortet omhändertas; jfr svårigheten att "återta" en nyckel som administreras så att den kan kopieras.

[6] Samtidigt måste effektiva rutiner för rapportering och registrering av förkomna kort finnas. En hotbild är rån, där rånaren också tilltvingar sig kortets kod, och därefter kan utföra digitala signaturer i annans namn. På sikt är det troligt att s.k. biometriska metoder — dvs. tekniska kontroller baserade på mätning av t.ex. fingeravtryck, röst, venmönster eller handgeometri — kommer att ersätta användningen av lösenord för verifiering av kortinnehavaren.

[7] Härvid kan många andra funktioner aktualiseras, t.ex. tidsstämpling av handlingar för att bereda skydd mot manipulationer med tidsangivelser.

som är helt identiska med dem som framställs i behörig ordning, och signering kan åtminstone under viss tid komma att ske utan att kortets rätta innehavare är medveten härom. Inte ens när kortinnehavaren t.ex. har avtvingats koden vet han vad som obehörigen signeras, och omfattande missbruk kan äga rum på kort tid.

Pappershandlingar med underskrifter som har tillkommit genom t.ex. tvång torde vanligtvis ge betydligt mer begränsat utrymme för missbruk. Det finns vedertagna rutiner för att undersöka manipulationer av pappershandlingar och personer med särskild kompetens för sådana undersökningar finns att tillgå. Motsvarande kompetens behöver finnas tillgänglig när någon ifrågasätter t.ex. en digitala signatur.

3.4 S.k. säkerhetstjänster på IT-området

Digitala signaturer kan användas också för andra funktioner än digitala underskrifter. Inom arbetet för internationell standardisering brukar dessa benämnas "säkerhetstjänster", och delas in i

- dataintegritet (content integrity),
- ursprung (origin authentication),
- inte förneka ursprung (non-repudiation of origin),
- inte förneka mottagande (non-repudiation of receipt),
- insynsskydd (confidentiality of content), och
- skydd mot duplikat (sequence integrity).

Flera säkerhetstjänster kan täcka varandra. Framställning av digitala dokument, dvs. med signatur, kan täcka de fyra första tjänsterna. Man kan säga att dataintegritet och ursprung får man "på köpet" när ett digitalt dokument skapas. Insynsskyddet innebär att krypteringsteknik används på det traditionella sättet för att förhindra att någon annan än den som är behörig (och därför känner krypteringsnyckeln) kan läsa dokumentets innehåll.

Skyddet mot duplikat är särskilt intressant där order m.m. skickas i mer eller mindre automatiserade processer. Detta skydd bygger på att man tillför dokumentet löpnummer eller tidinformation (s.k. time-stamp).

Digitala signaturer och liknande rutiner kan också användas för säkerhetsfunktioner utanför dokumentområdet, t.ex. för tillträdeskontroll och för att verifiera organisationer, befogenheter, enheter och processer.

3.5 Nuvarande tillämpningar

Rutiner baserade på digital signering har fått en omfattande spridning, och används idag bl.a. då betalningsuppdrag överförs via magnetband och disketter eller teletransmission till en bank eller ett giroinstitut och när tulldeklarationer sänds i form av digitala dokument från en näringsidkare till tullen. Sådana rutiner håller vidare på att införas inom

bl.a. skatteförvaltningen, exekutionsväsendet och polisen, för att möjliggöra IT-baserade ärendehanteringssystem och säker kommunikation.

Ett uppmärksammat EU-projekt, benämnt "Bolero", syftar till att skapa en ersättning för dagens hantering av konossement vid marina transporter. Den lösning som prövas innebär att man använder digitala dokument försedda med digitala signaturer enligt vad som beskrivits ovan, samt att en betrodd tredje part registrerar innehav av dessa dokument och i varje ögonblick har aktuell information om vem som innehar ett visst dokument. På så sätt kan det genom IT-rutiner visas inte bara att ett dokument är omanipulerat utan också vem som har rätten till visst gods.

Som ett annat exempel på sådana projekt kan nämnas den modell som en internationell arbetsgrupp har tagit fram, för att beskriva hur t.ex. betalningsuppdrag skall skyddas under transport och hur dagens skriftliga avstämningsuppgifter ska kunna bytas ut mot digitala dokument.[8] Modellen, som är generell vad gäller framställning och kontroll av digitala dokument, upptar — utöver funktioner för den beskrivna signeringen — tekniska och administrativa rutiner, varigenom den som tar del av en handling kan verifiera att uppgiften om utställare är riktig och att innehållet inte har manipulerats.

Vidare diskuteras frågan om att tillskapa en trovärdig tredje part (Trusted Third Party) som kan anförtros vissa funktioner som är särskilt betydelsefulla för säkerheten inom sådana rutiner, såsom att administrera hemliga nycklar och garantera deras äkthet och knytning till angiven person.

Inom ramen för ett nyligen avslutat projekt inom bankvärlden[9], har en specifikation utarbetats för elektroniska ID-kort. Specifikationen innefattar inte bara tekniska beskrivningar av funktioner för identifiering av kortinnehavaren, framställning av digitala signaturer och stöd för kryptering, utan också en beskrivning av de administrativa rutiner som krävs för att ett sådant kort ska kunna accepteras av övriga parter i projektet.

Ett ytterligare exempel på vilken vikt som läggs vid dessa säkerhetsfrågor och krav på samordning, är bildandet av den svenska intresseföreningen Säkrad Elektronisk Informationshantering i Samhället (SEIS). Ett femtiotal organisationer bestående av företag med många användare av datorsystem, implementatörer av programprodukter och

[8] Arbetet, benämnt EDIFACT FINANS, ingår i det av FN administrerade organet UN/EDIFACT, och bedrivs genom en samarbetsorganisation inom den finansiella sektorn, vars syfte är att utveckla standarder och gemensamma rutiner som ska underlätta utväxling av information inom världshandeln.

[9] Projektet "Strategisk samverkan kring elektroniskt ID-kort", i vars styrgrupp Handelsbanken, Nordbanken, S-E-Banken, Sparbanken, Posten, Ikano Finans, Smart och Telia har medverkat.

leverantörer av maskinvaror har redan slutit upp bakom föreningen, vars syfte är att genom samverkan mellan medlemmarna påskynda utvecklingen av nya standarder inom IT-säkerhetsområdet.

Produkter som stöder digitala signaturer finns också på marknaden. Utvecklingen befinner sig emellertid i ett inledande skede och från rättslig utgångspunkt knyts intresset till de beskrivna grundläggande funktionerna, inte till valet av specifika tekniska lösningar.

4 Närmare om kryptering

De beskrivna säkerhetstjänsterna bygger, om man bortser från skyddet mot duplikat, på användning av krypteringsteknik. Detta kan förklaras på följande sätt.

Krypto, från grekiskans *kryptos*, som betyder dold, hemlig, har tidigare varit förknippad med militärens bruk av system för att förvränga text eller tal och på så sätt skydda information mot åtkomst utanför de invigdas skara. Dagens användning av krypteringsalgoritmer och tillhörande nyckeladministration, bygger på matematisk vetenskap och sannolikhetslära.

De båda världskrigen, det "kalla kriget", ett tilltagande industrispionage och ökad konkurrens som har aktualiserat olika former av affärsunderrättelseverksamhet, har inneburit en kraftig utveckling inom kryptografins område under 1900-talet. Då information inom IT-området alltid kan brytas ned till digitala signaler framstår krypteringstekniken som det naturliga sättet att skydda elektroniskt hanterad information.[10]

Krypteringsalgoritmer används numera för två olika syften. Dels används tekniken för att säkerställa att innehållet i en datamängd inte har rubbats eller förändrats (dataintegritet). Detta innebär en förhöjning av datas kvalitet och är förutsättningen för att kunna skapa digitalt signerade dokument. Dels används kryptering för att skydda mot insyn (konfidentialitet). Detta senare användningsområde har fört med sig en intressekonflikt mellan å ena sidan myndigheter och företag som vill skydda sin information och å andra sidan det intresseområde som rör rikets försvar och säkerhet i övrigt. I vissa länder har användning av kryptering som inte kan brytas av egna myndigheter förbjudits.

De krav som tidigare ställdes på västvärldens länder via COCOM (Committee for Multilateral Export Controls), ersattes nyligen av "New Forum" och Sverige har i lagen (1991:341) om strategiska produkter och förordningen (1994:2060) om vissa strategiska produkter, föreskrivit vissa exportbegränsningar. Regleringen baseras på ett EG-direktiv.

[10] För närvarande är detta enda sättet att "frysa" informationen till ett mönster eller en bild för att på så sätt skapa en kontroll som innebär att om "data-bitarnas" inbördes placering förändras, kan detta upptäckas.

Det finns emellertid inga hinder mot att importera eller använda krypteringmetoder i Sverige.

De som vill försvara en statlig kontroll av kryptografiska metoder hänvisar till behovet av information för att förebygga hot mot rikets säkerhet och brott såsom terrorism och narkotikahandel. Eftersom effektiva användarvänliga säkerhetstjänster numera finns tillgängliga på den öppna marknaden blir det emellertid allt svårare att undanhålla den laglydiga delen av en nation säkerhetstjänster som alltfler uppfattar som en slags rättighet, och som dessutom är avgörande för utvecklingen på IT-området.

Det civila behovet av fri tillgång till säkerhetstjänster som utnyttjar "bästa möjliga teknik", har uppmärksammats av flera organisationer. TeleTrusT Sverige reagerade tidigt mot lösningar med inbyggda "bakdörrar" för vad som brukar kallas "legal avlyssning". Man hänvisade till att sådana system inte kommer att kunna åtnjuta förtroende och att användare därför skulle addera egna lösningar för att skydda sin information. Detta skulle i sin tur kunna leda till totalt förbud för användning av egna skyddstjänster.

Internationella Handelskammaren, ICC, har utarbetat ett "Position Paper" som nu finns tillgängligt i organisationens nationella kommittéer i mer än 100 länder. I detta uppmanas regeringarna i respektive land att undanröja alla hinder för att införa och använda säkerhetstjänster baserade på kryptografiska metoder. Svenska ICC har riktat denna uppmaning direkt till Kommunikationsdepartementet. Andra organisationer som agerat i denna fråga är Bankföreningen som begärt att ESEK (Enheten för strategisk exportkontroll vid UD) skall agera för att minimera de problem som uppstått på grund av den nya lagstiftningen och verka för att politiska förutsättningar skapas som leder till lagändring och undanröjande av nuvarande hinder.

Den nyligen skapade intresseföreningen SEIS (Säkrad Elektronisk Informationshantering i Samhället) har hos samordningsministern begärt att de politiska frågorna inom detta område skall lyftas fram eftersom dessa är avgörande för IT-utvecklingen från internationellt perspektiv.

För elektronisk dokumenthantering inom Sverige finns alltså inga rättsliga hinder mot att använda kryptografiska metoder, oavsett om man önskar uppnå skydd mot olovlig insyn eller skydd för en handlings äkthet. Internationellt behöver emellertid frågan om kryptering få en politiska lösning i samarbete med övriga länder, såväl inom EU som på global nivå.[11] IT-utvecklingen är i hög grad internationell och digitala signaturer och stämplar samt tekniska insynsskydd behöver följa informationen även när data sänds mellan olika länder. Det behövs alltså tillgång till väl fungerande rutiner för kryptering samt anknytande

[11] En expertgrupp planeras inom OECD för att överväga frågor om krypteringspolicy.

hård- och mjukvaror. Situationen blir annars den att myndigheter och företag kan nyttja sina informationssystem internationellt endast om de övergår till metoder som inte fyller rimliga krav på informationssäkerhet.

1 Arkiv — bevarande och gallring

1.1 Allmänt

Den teoretiska grunden för arkivverksamheten i Sverige har sedan början av 1900-talet varit den s.k. ursprungsprincipen. I enlighet med detta betraktelsesätt utgör en handling ett led i ett händelseförlopp. Handlingens värde är beroende av möjligheterna att kunna fastställa handlingens ursprung och dess samband med andra handlingar.[12] Mina förslag är inte oförenliga med detta synsätt.

Den traditionella arkivteorin har utgått från ett bevarande av fysiska enheter och strukturer. En myndighets ärendehandläggning har kunnat speglas genom ett bevarande av handlingarna i en bestämd fysisk ordning. Med dagens teknik ersätts den fysiska ordningen i allt högre grad av logiska samband. Se vidare om elektroniska akter m.m. i bilaga 6. Vidare har ett bevarande av de fysiska handlingarna fått ersättas av ett bevarande av informationsinnehållet genom överföring till nya databärare och medier.

Från arkivsynpunkt kan en handling sägas bestå av data som finns på en databärare. Därtill kommer en rad egenskaper som är förknippade med de medel och metoder som har valts för handlingens framställning, representation, bearbetning, överföring, presentation, läsning, lagring m.m. Valet av medium för med sig såväl möjligheter som begränsningar i hantering och användning av informationen.

Övergången till IT har, som tidigare sagts, medfört att information bevaras genom överföring - från hårddisk till bandkassett, från papper till optisk skiva etc. När bevarande sker på detta sätt blir rutiner och kontroller i samband med överföringen avgörande för om läsbarhet och övriga kvaliteter hos handlingarna skall kunna bevaras.

Risker för informationsförluster finns vid alla slags överföringar av handlingar. Om sådana överföringar fick göras okontrollerat skulle informationsförluster säkerligen uppkomma för den som vill ta del av ett nytt exemplar. Enligt min mening måste myndigheterna i varje enskilt fall ta ställning till vad som händer vid överföring av data till en annan databärare. Överföringen kan medföra sådana informationsförluster att de ursprungliga handlingarna inte får förstöras.[13]

Långtidslagring av elektroniska handlingar ställer andra krav på myndigheterna än det traditionella arkivmaterialet. För att läsbarheten hos handlingarna inte skall gå förlorad krävs att de framställs med materiel och metoder som medger konvertering och överföring till nya

[12] Om det är möjligt att fastställa vem som är utställare till en viss handling kan även informationens kvalitet och källvärde bedömas.

[13] Överföringar mellan *digitala* databärare behöver inte ge dessa förluster, meden traditionell kopiering av pappershandlingar eller utskrift av data på papper eller mikrofilm som regel ger sådana förluster.

databärare under hela bevarandetiden. Härutöver krävs en tillfredsställande systemdokumentation. Om möjligheten att äkthetspröva digitala dokument skall vidmakthållas behöver också nycklar och algoritmer bevaras.

För att tillgodose arkivlagens syften har Riksarkivet utfärdat verkställighetsföreskrifter på området. Därav framgår bl.a. att all förstöring av allmänna handlingar och uppgifter i allmänna handlingar utgör gallring. Detta gäller även om data dessförinnan har överförts till en ny databärare om överföringen medför förlust av information eller sökmöjligheter eller av möjligheter att fastställa en handlings autenticitet. Sådana åtgärder får alltså inte vidtas utan särskilt beslut, som har stöd i lag, förordning eller myndighetsföreskrifter. Vidare har det införts krav på rutinerna för överföring av handlingar mellan olika databärare, i syfte att minimera förlusterna av läslighet m.m. Nuvarande regler hindrar emellertid inte en övergång till elektronisk post, elektroniska akter etc.

Gallring är en praktisk nödvändighet som syftar till att begränsa arkivens omfattning, men även till att arkiven inte skall tyngas av handlingar som saknar påtagligt informationsvärde. Som tidigare sagts (avsnitt 6.4) får myndigheterna enligt 10 § arkivlagen avhända sig allmänna handlingar genom gallring.

Vid sidan av den gallring som sker av hanterlighetsskäl och ekonomiska skäl, har användningen av automatisk databehandling aktualiserat en gallring som är påkallad av helt andra skäl, nämligen integritetsskyddet för den enskilde. Föreskrifter om gallring finns i flera registerlagar. Vidare kan Datainspektionen med stöd av datalagen meddela föreskrifter om gallring. En avvägning mellan arkivlagens och datalagens syften kommer till stånd genom de samråd som äger rum mellan Riksarkivet och Datainspektionen.

1.2 Konkurrerande regler rörande gallring

Det har blivit vanligt att uppgifter bevaras både på papper och elektroniskt genom att vissa uppgifter i pappershandlingar förs in också i ett egentligt register hos en myndighet. När elektroniska akter införs och pappersbaserat material scannas kan det till och med förekomma att samma uppgift finns på papper, i den elektroniska akten samt i myndighetens egentliga register.[14] Vid sådan dubbel- eller trippellagring behöver det beaktas att bestämmelser om gallring finns såväl i arkivförfattningarna som i datalagen och vissa andra författningar, samt att *olika gallringsfrister* kan gälla för det pappersbaserade materialet

[14] Jfr Ds 1994:80 s. 90 och 143.

respektive för myndighetens register.[15] En kort gallringsfrist kan ha föreskrivits för uppgifterna i registret eftersom pappershandlingarna skall bevaras.

Ändringar av gallringsregler i registerförfattningar som är svåra att förena med en övergång till elektronisk akthantering, kan dock knappast övervägas utan närmare kännedom om de rutiner som avses införas på olika områden. Jag vill därför endast erinra om vikten av att uppmärksamma dessa frågor i samband med att nya rutiner införs för elektronisk kommunikation och elektronisk akthantering.[16]

1.3 Bevarande av ingivna databärare?

Det kan antas komma att bli vanligt att disketter och andra ADB-medier ges in till myndigheter. Valet av rutiner för att ge in data till en myndighet har betydelse för frågan om hur inkommet IT-material bör bevaras och gallras — bör själva bäraren med data bevaras eller bör data läsas över till myndighetens databärare?

En överföring mellan databärare innebär i vissa fall endast försumbara förluster. I sådana fall kan de ursprungliga handlingarna gallras, i enlighet med Riksarkivets föreskrifter och allmänna råd om gallring av handlingar av tillfällig eller ringa betydelse.[17] Byte av medium innebär dock vanligtvis sådana förluster att det krävs särskilda gallringsföreskrifter. Medgivande till gallring av ursprungshandlingarna efter överföring knyts till krav på kompenserande åtgärder vid överföringen. Det kan t.ex. gälla krav på upprättande av sökingångar till de överförda handlingarna eller vidimering och stämpling av handlingarna efter kvalitetskontroll. Krav av detta slag ingår i Riksarkivets mediespecifika regler.

Från praktisk utgångspunkt är det också svårt att motivera ett bevarande av alla de databärare som ges in med skilda format, teckenrepresentationer, etc. En myndighet kan knappast under någon längre tid ha alla de hård- och mjukvaror tillgängliga som behövs för att kunna göra samtliga mottagna databärare läsbara. Vidare torde huvuddelen av de databärare som ges in inte vara godkända för lagring av data under någon längre tid, och ett bevarande av dessa bärare är ut-

[15] Jfr angående skatteförvaltningens dokumenthantering, Ds 1994:80 s. 89 f. och 139 f., prop. 1994/95:93, bet. 1994/95:SkU15 och rskr. 1994/95:158, och beträffande kronofogdemyndigheternas indrivningsverksamhet Finansdepartementets promemoria den 22 december 1994, Nytt ADB-stöd för indrivningsverksamheten, Fi94/2903, prop. 1994/95:168, bet. 1994/95:LU27, rskr. 1994/95:305.

[16] Eftersom en förstöring av pappersmaterial, efter att det har scannats, vanligtvis medför viss förlust av möjligheten att fastställa informationens äkthet, medan en förstöring av elektroniskt material ger viss förlust av sökmöjligheter, föreligger gallring när den ena lagringsformen förstörs oavsett vilket alternativ som väljs.

[17] Ett sådant synsätt torde tillämpas också beträffande räkenskapsmaterial enligt 10 § första stycket 3 bokföringslagen (1976:125).

rymmeskrävande. Om myndigheten löser dessa frågor kvarstår de komplikationer som följer av att delar av materialet på en viss databärare kan ha en kortare gallringsfrist än återstoden.

Tanken att ingivna databärare skall bevaras torde delvis ha sin grund i att detta är självklart i pappersmiljö. Beträffande IT-material brukar, som hinder mot överföring till myndighetens databärare, nämnas faran för maskinella fel vid läsningen till den nya databäraren. Risken för sådana tekniska fel är dock obetydlig med nuvarande teknik. Att förändringar av data därvid också slumpvis skulle generera en felaktig siffra eller bokstav som under handläggningen framstår som korrekt är synnerligen osannolikt. Det traditionella synsättet, att det ingivna originalet bör bevaras, har som framgått inte sådan bärkraft i IT-miljön att säkerheten bör knytas till ett visst fysiskt föremål.[18]

Argumenten för att bevara ingivna databärare blir ännu svagare när det beaktas hur disketter och andra datamedier sänds med post och i övrigt förvaras under sådana former att man inte kan bortse från risken för manipulationer. Vid förvaringen följs visserligen de regler som gäller för annat material såsom pappershandlingar, men de elektroniska handlingarna kan manipuleras enklare och i det närmaste spårlöst. Rutiner där databärare ges in till en myndighet utan att data är låsta med någon teknisk kontrollmetod har alltså brister från säkerhetssynpunkt som ett bevarande av själva databäraren inte kan avhjälpa. På sikt torde de berörda frågorna komma att lösas genom att samtliga elektroniska handlingar förses med digitala signaturer eller digitala stämplar, oberoende av om de ges in via nät eller genom att en databärare inges. Rutiner förekommer också, t.ex. inom tullen och skatteförvaltningen, där dessa brister har beaktats genom att tekniska kontrollrutiner har knutits till själva data.

Det bör alltså krävas att myndigheterna bevarar inkomna elektroniska handlingar på databärare som är godkända för långtidslagring — men inte nödvändigtvis på ingivna databärare — och att myndigheterna säkerställer att data inte oavsiktligt eller avsiktligt förändras. Riskerna för fel vid läsningen från en databärare till en annan bör begränsas genom tekniska kontrollåtgärder. Vidare krävs anpassningar till den tekniska och administrativa verkligheten så att mottagna elektroniska handlingar bevaras säkert, och med en sådan struktur att rättskipningens, förvaltningens och forskningens behov samt enskildas rätt att ta del av handlingar tillgodoses. Den närmare utformningen av rutinerna är dock av sådan detaljkaraktär att frågan inte behandlas närmare i detta sammanhang.

[18] Det föreligger endast ett original*innehåll* eftersom data som representerar en handling på en viss databärare, med nuvarande tekniska metoder, knappast kan skiljas från samma mönster av elektroniska signaler på en annan bärare.

1.4 Överföringar mellan medier — vidimering

Utöver tekniska kontroller för att säkerställa att data oförvanskat läses över till en ny databärare är det av intresse att kunna få besked om vem som har utfört arbetet. Sådana upplysningar kan vara betydelsefulla om materialets äkthet ifrågasätts vid t.ex. myndigheten eller en domstol. Därför upprättas vanligtvis protokoll över vidtagna åtgärder.[19] En naturlig utveckling är dock att, i analogi med vidimering av avskrifter och fotokopior, använda digitala signaturer eller digitala stämplar, eventuellt i förening med en förklaring av den som vidimerar att data i enlighet med använda kontrollrutiner har överförts oförändrade till den nya bäraren.

Sådana rutiner kan också användas när elektroniska handlingar utan signatur/stämpel mottas via nät. Om handlingarna signeras/stämplas så snart de når mottagaren kan det kontrolleras om data därefter har förvanskats. På motsvarande sätt kan pappershandlingar scannas och signeras, samtidigt som det till den digitala bilden knyts en förklaring att den överensstämmer med det pappersbaserade originalet.

Från rättslig utgångspunkt innebär en vidimering av en pappersbaserad kopia av en urkund att också kopian anses vara en urkund enligt 14 kap. 1 § andra stycket BrB — den som vidimerar står som ett slags garant för handlingens bevisfunktion.[20] Om den som vidimerar sanningslöst intygar att kopian överensstämmer med originalet kan ansvar för osant intygande aktualiseras (15 kap. 11 § BrB). Om i stället annan ändrar i den vidimerade kopian eller om den som vidimerar tecknar annans namn, kan förfarandet vara att bedöma som urkundsförfalskning (14 kap. 1 § BrB). Är kopian inte vidimerad kan missbruk av urkund föreligga, om någon sannigslöst utger den för att vara en riktig kopia av en viss urkund (15 kap. 12 § BrB). Det är dock oklart om elektroniska handlingar — oberoende av om de har försetts med digital signatur — kan vara att bedöma som urkunder i brottsbalkens mening.[21]

[19] Detta är också förenligt med Riksarkivets krav på överföring för långtidslagring av IT-material, där det sägs att en överföring till annan databärare skall dokumenteras. Det skall även dokumenteras vilken operatör som har gjort överföringen (RA-FS 1994:2, 5 kap. 1 § och 3 kap. 6 §).

[20] Beckman m.fl., Brottsbalken II, 6 u., s. 73.

[21] Att gränsdragningen mellan falska resp. endast osanna urkunder — grundad på en bedömning av ett visst fysiskt originalexemplar — knappast kan tillämpas på elektroniska handlingar, har närmare utvecklats av Datastraffrättsutredningen, som föreslagit en reglering anpassad till datas karaktär, se vidare SOU 1992:110 s. 229 f., jfr s. 315.

1.5 Skall scannade pappersurkunder gallras?

I lagstiftningsärendet rörande elektronisk dokumenthantering inom skatteförvaltningen aktualiserades frågan om ingivna pappersurkunder bör gallras efter att de har scannats och tillförts en elektronisk akt. Frågan är inte enkel att besvara eftersom den har anknytning till många olika skyddsintressen. Utifrån intressen av t.ex. en rationell dokumenthantering och bevaring av uppgifter för framtida forskning framträder knappast några hinder mot att gallra originalen. Motsatt bedömning kan emellertid göras från rättssäkerhetssynpunkt och när samhällets intresse av att kunna utreda och beivra brott ställs i förgrunden. Det är betydelsefullt att också kunna tillgodose kraven på informationssäkerhet samt på parts- och offentlighetsinsyn.

Vid remissbehandlingen av en framställning från Riksskatteverket till regeringen angående elektronisk ärendehandläggning betonades från flera håll att pappersbaserade handlingar som scannas bör bevaras och vid behov kunna sökas fram. Frågan föranledde vidare Rikspolisstyrelsen att sända ut en förfrågan till vissa polismyndigheter angående möjligheterna att utreda och styrka brott på skatteområdet, för den händelse de skriftliga originalhandlingarna skulle komma att gallras efter att ha scannats. Polismyndigheterna i Stockholm, Göteborg och Malmö betonade vikten av att från brottsutredningssynpunkt bevara originalhandlingarna, bl.a. för de fall där namnteckningens eller innehållets äkthet ifrågasätts och för spårsökning.[22]

Rikspolisstyrelsens förfrågan besvarades också av Statens Kriminaltekniska Laboratorium, som uttalade att den viktigaste förutsättningen för att en handstilsanalys skall kunna komma till stånd är att den ifrågasatta handlingen föreligger i original, medan kravet på jämförelsematerial inte är lika högt ställt. Laboratoriet påpekade vidare att det — om originalen förstörs — inte längre finns möjligheter till undersökning av ingrepp och ändring, bläckanalys, maskinskriftsundersökning, pappersanalys, m.m.

Enligt min mening finns inte nu underlag för någon allmän bedömning av huruvida gallringen av pappersurkunder kan tidigareläggas, när samma uppgifter finns i elektroniska akter. Nya metoder utvecklas snabbt på området, och det är oklart hur de närmare rutinerna för hantering av pappersbaserat materialet som har scannats kommer att utformas och vilket behov av åtkomst till originalhandlingarna som kommer att föreligga vid t.ex. överklaganden. Till detta kommer de uppgifter Statens Kriminaltekniska Laboratorium och vissa polismyndigheter har lämnat angående vikten av att bevara originalexemplaren. Dessa bör därför — i vart fall så länge de praktiska förut-

[22] Vidare anförde polismyndigheten i Malmö dels att det bör införas någon form av vidimering genom vilken intygas att den elektroniska bilden överensstämmer med originalet, dels att den som utfört scanningen bör vara identifierbar.

sättningarna för att söka fram pappershandlingar och äkthetspröva elektroniska handlingar inte har klarlagts — registreras och arkiveras så att de enkelt kan återfinnas. Myndigheterna har härefter att, vid en samlad avvägning mellan motstående intressen av bl.a. säkerhet och effektivitet, bedöma om och i så fall efter hur lång tid gallring bör kunna ske av pappersbaserade handlingar som har scannats. Som tidigare nämnts är det inte heller tillåtet för myndigheterna att gallra de ursprungliga handlingarna utan särskilda föreskrifter.

1.6 Långtidslagring av digitala dokument

Redan när en övergång till elektronisk dokumenthantering aktualiseras behöver det övervägas hur långtidslagring skall ske om äkthetsprövning och omvandling till klartext av krypterat material avses kunna ske med bibehållen säkerhet många år senare. Hur bör myndigheterna hantera hemliga nycklar för signering och kryptering och hur bör myndigheterna möta matematiska framsteg eller andra förändringar som kan göra det möjligt att forcera tekniska säkerhetsrutiner? Dessa frågor bör dock övervägas för varje enskilt fall. Det är varken lämpligt eller möjligt att lagreglera sådana tekniska och snabbt föränderliga förutsättningar.

På motsvarande sätt bör myndigheterna noga överväga de komplikationer som kan framträda i blandade miljöer, dvs. när handlingarna i ett ärende delvis förvaras elektroniskt, delvis på papper.

Rättsliga "standarder"

Användningen av IT förutsätter att alla uppgifter och instruktioner bryts ned till elektroniska operationer. Därför krävs entydiga rutiner för varje enskild åtgärd; jfr förfarandet när det gäller användningen av pennor, färgband, papperskvaliteter och annan skrivmateriel i myndigheternas verksamhet.[23]

I doktrinen har föreslagits att behoven av att stärka rättssäkerheten och att nedbringa kostnaderna för myndigheternas IT-användning delvis skall tillgodoses genom rättsliga "standarder", dvs. modellösningar som ger underlag för en ökad integration av juridik och IT i den offentliga förvaltningen.[24] Sådana åtgärder — inriktade på en viss funktionalitet — anses kunna fungera som en brygga mellan myndigheternas tekniska miljöer och rättsreglerna på området, så att myndigheternas utveckling och användning av IT därmed kan befordras generellt, utan att varje detalj måste lösas separat för varje verksamhet eller ärendekategori.

Jag ansluter mig till denna bedömning. Med hänsyn till teknikutvecklingen och myndigheternas ökande utnyttjande av IT framstår det som angeläget att på detta sätt kunna utforma rättsliga funktionalitetskrav på områden som inte varit föremål för särskild uppmärksamhet i detta avseende. Beträffande det IT-baserade förvaltningsförfarandet handlar det bl.a. om hur utformning och motivering av automatiskt genererade beslut bäst kan ske, liksom tekniska lösningar för att realisera bestämmelser om dokumentationsskyldighet, med beaktande av kraven på en rationell process för elektronisk ärendehandläggning. I stället för att varje gång "uppfinna hjulet" på nytt bör således vedertagna modeller kunna användas för vissa frågor och rutiner av generell natur. Genom att utforma dessa modeller som förebilder för vad som kännetecknar en god verksamhet bör bedömningen av vad som är acceptabelt respektive oacceptabelt från juridisk synpunkt kunna förenklas. Detta gäller såväl för den som utvecklar ett nytt informationssystem som för en myndighet eller en domstol som har att pröva rättsfrågor som uppkommer inom ramen för en IT-rutin, jfr den

[23] Statliga myndigheter skall, i enlighet med RA-FS 1994:1, använda skrivmateriel som är certifierad för överensstämmelse med Riksarkivets tekniska krav. Alternativt accepteras en leverantörsförsäkran. Reglerna är anpassade till europeiska standarder (SS-EN 45 000-serien). När det gäller ADB-användning är beständigheten beroende av lämpliga standardiserade format för data, dokumentation av hanteringen samt goda rutiner och hög säkerhet vid överföring, konvertering och lagring av data, se de föreskrifter för bl.a. ADB-området som Riksarkivet från och med den 1 juli 1991 har utfärdat med stöd av arkivförordningen.

[24] Cecilia Magnusson Sjöberg, Rättsautomation, s. 509 f. och 524 f.

betydelse säkerhetsföreskrifter i traditionell miljö har vid prövningen av frågor om skadestånd m.m.[25]

Utformningen av rättsliga standarder kan med andra ord bidra till att IT-anpassa den offentliga förvaltningen utan ingrepp i befintliga regelverk. Väl utformade kan de befordra rättssäkerheten och ge nya möjligheter att kostnadseffektivt utveckla informationssystem. Vidare torde prövningen av vissa rättsfrågor kunna förenklas genom en sådan metod.

Ett sådant samspel mellan standarder och föreskrifter utgör inte någon ny företeelse i Europa.[26] Som ett led i strävandena att effektivisera harmoniseringsarbetet i EG antog EG-rådet år 1985 en resolution om en ny harmoniseringsteknik — "the new approach". Där anges hur det i direktiv kan hänvisas till Europeiska standarder. Direktiven skall innehålla endast grundläggande säkerhetskrav. Dessa skall sedan automatiskt anses vara uppfyllda om en viss vara tillverkats enligt harmoniserade europastandarder. Utvecklingen har fortgått i riktning mot myndighetsregler harmoniserade via standarder.[27]

[25] I sammanhanget bör nämnas att den expertis som krävs för att lösa olika detaljfrågor av betydelse för rutinerna i IT-miljön, inte finns inom varje myndighet, och att frågornas omfattning och komplikationsgrad medför att det inte är realistiskt att myndigheterna, i alla delar, utformar t.ex. verkställighetsföreskrifter eller allmänna råd eller fattar beslut för enskilda fall i varje detaljfråga.

[26] Som exempel kan nämnas EG:s s.k. lågspänningsdirektiv från 1973 där det, för att uppfylla direktivens allmänna säkerhetskrav, hänvisas till vissa standarder. EG:s verksamhet för att undanröja tekniska handelshinder inriktades från början mot att i direktiv i detalj ange de krav som skall gälla för berörda varor. Medlemsländerna har därefter haft att införa dessa krav i sina nationella författningar.

[27] Se vidare Europastandardiseringens betydelse för Sverige och för integrationen i Västeuropa, Fakta Europa 1989:2 s. 10 f.

Elektronisk adressering, postöppning och diarieföring

Frågan om en regleringen av inkommande elektroniska handlingar har ett nära samband med hur rutinerna för elektronisk adressering utformas. Mitt förslag bygger på att myndigheter och enskilda kan skilja elektroniska myndighetsadresser från privata eller annars personliga elektroniska adresser.

I traditionell miljö är det självklart vad som utgör en myndighetsadress, och besked härom lämnas på vedertaget sätt via telefonkataloger, myndighetens brevpapper, etc. Elektroniska adresser har emellertid i huvudsak kommit att knytas till individer, så att det ofta framstår som oklart vilka elektroniska adresser som innehas i tjänsten. En tjänsteman kan ha en egen elektronisk adress, t.ex. genom ett privat avtal med ett företag som förmedlar uppkopplingar till Internet, jfr den traditionella brevlådan vid bostaden.[28] Vidare kan arbetsgivaren bereda en tjänsteman tillgång till en mängd uppkopplingar mot olika informationssystem. Härvid är det snarare regel än undantag att olika tjänster i skilda informationssystem har kombinerats med funktioner för elektronisk post, så att en tjänsteman för varje enskilt fall tilldelas ytterligare en adress för elektronisk post — trots att varken tjänstemannen eller myndigheten vill ha denna tjänst. Andra exempel på elektroniska adresser som inte är avsedda för kommunikation med myndigheter i mål och ärenden är internetuppkopplingar som tekniskt ansvariga vid myndigheter har endast för att ta del av teknisk information och att hämta programvaror m.m.

Samma ordning och reda som vid adressering i traditionell miljö bör naturligtvis gälla också i IT-miljön. Det bör därför bestämmas vilka elektroniska adresser en viss myndighet har och dessa adresser bör, såsom vanligtvis sker med traditionella adresser, anges på brevpapper, visitkort etc.

När privata adresser och telefaxnummer sätts ut på t.ex. visitkort anges regelmässigt att de avser bostaden. Även om arbetsgivaren i ett visst fall äger en telefaxapparat i en tjänstemans bostad och betalar telekostnaden torde en handling som når denna adress inte anses vara inkommen i processuell mening förrän den har kommit tjänstemannen till handa eller har transporterats till myndigheten, trots att myndigheten tillhandahållit denna möjlighet till kommunikation.

Detsamma bör enligt min mening gälla för e-postadresser. Det är inte realistiskt att kommunikationsleder som inte har varit avsedda för

[28] Det bör som sagt inte krävas att tjänstemannen tömmer denna brevlåda varje dag, eller att han i samband med t.ex. semestrar lämnar ut sitt lösenord till arbetsgivaren för att denne skall kunna kontrollera om det bland den privata elektroniska posten finns något meddelande som rör tjänsten.

kontakter mellan myndigheter och enskilda i mål eller ärenden, skall behandlas som om de hade ett sådant syfte.

Det är alltså en betydelsefull fråga hur elektronisk adressering går till och hur myndigheterna tillhandahåller sina elektroniska adresser.[29] Myndigheterna måste se till att det går att skilja mellan myndighetsadresser respektive privata adresser och adresser som visserligen tillhandahålls i tjänsten men för andra syften än kontakter mellan myndigheten och enskilda. Detta hindrar naturligtvis inte att myndighetsadresser utformas så att också en viss tjänsteman pekas ut, jfr vanliga kuvert där det under myndighetens namn ofta anges "Attention N.N.".

Jag har i mina förslag utgått från att myndigheterna kommer att tillgodose behovet av rättssäkra rutiner, genom att tydligt ange vilken eller vilka elektroniska adresser en viss myndighet har, och att administrera övriga elektroniska adresser så att rättsförluster för enskilda inte uppkommer. Därmed behövs ingen lagreglering utöver bestämmelser om när en elektronisk handling skall anses ha kommit in.[30]

Denna syn på adresseringen innebär att en elektronisk handling kan anses inkommen enligt bestämmelserna i 2 kap. TF, trots att den inte anses vara inkommen enligt regleringen i RB, FL och FPL. Det betydelsefulla i detta sammanhang är emellertid att rättsförluster kan undvikas för den som sänder en handling till myndighetens elektroniska adress, genom att en handling som inte anses inkommen enligt TF därför att myndigheten saknar tekniskt hjälpmedel för läsningen, anses inkommen enligt den processuella regleringen.[31]

Härvid bör betonas vikten av att undanröja de risker som en illa vald IT-användning kan föra med sig både för rättssäkerheten och för skyddet av den enskildes personliga integritet.[32]

För pappersmiljön finns vedertagna rutiner för postöppning och diarieföring, och olika åtgärder har vidtagits vid domstolar och förvaltningsmyndigheter i syfte att underlätta arbetet för de tjänstemän som tar befattning med inkommande post.[33] I IT-miljön behövs på motsvarande sätt ordnade rutiner för postöppning och diarieföring. Det är härvid betydelsefullt med väl genomtänkta rutiner för bl.a. adressering.

[29] Regeringen har, som framgått, tillsatt en utredning rörande behov av en nationell teleadresskatalog (dir. 1995:125). Utredningen syftar emellertid till att i nuvarande struktur hålla adresser tillgängliga, inte till att se över formerna för denna adressering.

[30] Motsvarande frågor aktualiseras vid telefaxkommunikation. Utvecklingen går mot att fax kan sändas direkt till en tjänstemans dator. Det förekommer vidare att flera telefaxapparater placeras ut hos en myndighet, trots att bevakning och administration av inkomna meddelanden inte motsvarar de krav som ställs på myndighetens traditionella posthantering.

[31] Även om data som representerar en handling har nått fram till myndigheten, anses handlingen enligt 2 kap. 3 § TF inte vara förvarad hos myndigheten om den inte är tillgänglig för myndigheten med tekniskt hjälpmedel som myndigheten själv utnyttjar för överföring i sådan form att den kan läsas, avlyssnas eller på annat sätt uppfattas.

[32] Se Seipel i Juridisk Tidskrift, årgång 5, s. 374 f. och SOU 1992:110, bl.a. s. 306 f.

[33] Se bl.a. Hellners/Malmqvist, Nya förvaltningslagen, 4 u., s. 110.

De strukturer som skapas bör tillgodose såväl rättsliga som administrativa intressen. Därför behöver både myndigheter och funktioner vid myndigheter kunna anges som adressat.[34]

När den elektroniska posten är adresserad till en viss handläggare aktualiseras frågan om vem som bör få öppna elektronisk post som når myndigheten. En fråga är om viss post bör ses som privat, jfr att vanliga postförsändelser oftast inte öppnas av myndigheten om adresseringen på kuvertet har utformats så att en viss handläggares namn står före myndighetens namn.[35] Följande påhittade internetadresser kan förtydliga frågan.

> Myndigheten (i detta exempel Göteborgs tingsrätt = gbgtr) har en egen server knuten till Internet med adressen gbgtr.se (se=Sverige). All post går således direkt till tingsrätten. Får registrator hos rätten, utan samtycke av rådmannen Jan Jansson, öppna e-post ställd till Jansson på adressen jan.jansson@gbgtr.se, eller bör det för postöppning utan samtycke krävas att adresseringen utformas så att myndighetens namn står först (**gbgtr**.jan.jansson@gbgtr.se)?[36] Bör samma synsätt gälla om myndigheten inte har någon direkt knytning till Internet utan abonnerar på en elektronisk brevlåda hos t.ex. Tele2? Adressen blir därvid, efter @-tecknet, mailbox.swipnet.se. Får registrator i detta fall utan samtycke öppna e-post adresserad direkt till Jan Jansson (jan.jansson @mailbox.swipnet.se) eller måste adresseringen, för att central postöppning skall vara tillåten, först uppta myndighetens namn (**gbgtr**.jan.jansson@mailbox.swipnet.se)?[37]

Utgångspunkten är att e-post skall vara ett medel att effektivisera förvaltningen och förenkla enskildas kontakter med myndigheter. En privat användning av sådana rutiner på arbetsplatsen kan föra med sig både rättsliga och administrativa komplikationer vid t.ex. diarieföring och utlämnande av allmänna handlingar. Statskontoret m.fl. myndigheter har därför förbjudit privat användning av myndighetens e-postsystem, med stöd av den allmänna principen att myndighetens medel får användas endast för myndighetens verksamhet.

En myndighet kan emellertid i praktiken inte hindra att privata e-postmeddelanden kommer in via myndighetens elektroniska brevlådor, jfr vanliga telefonsamtal. Det är inte heller prövat om myndigheten genom ett förbud mot privat användning kan förfoga över olovlighetsrekvisiten i 4 kap. 8 § BrB och 21 § DL, så att meddelanden som någon sänder till en tjänsteadress får läsas utan samtycke av adressaten. Därför bör myndigheterna, när e-post och andra sådana externa kommunikationsleder ställs till tjänstemännens förfogande, göra klart genom t.ex. interna föreskrifter och överenskommelser med de anställda vad som gäller i olika avseenden, t.ex. att myndigheten får "öppna"

[34] Jfr RH 1991:3 ang. risken för rättsförluster vid felaktig adressering.

[35] Se vidare JO:s beslut den 31 januari 1994, dnr. 4-1993, med hänvisningar.

[36] Jfr adresseringen jan.jansson.**gbgtr**@gbgtr.se.

[37] Jfr X 400-adresser som har en helt annan uppbyggnad.

inkommande post i den omfattning som behövs för att undvika rättsförluster, t.ex. när en tjänsteman är bortrest eller sjuk.

En annan fråga rör hur rutinerna för diarieföring bör utformas. Det kan vara rationellt att elektronisk post och telefaxmeddelanden adresseras direkt till berörd handläggare. Härvid aktualiseras emellertid behovet av fungerande rutiner för diarieföring, t.ex. så att handläggaren med ett enkelt kommando kan ange om diarieföring skall ske, eller så att elektronisk post som har adresserats till enskilda handläggare med automatik kan kopieras och vidarebefordras till registrator. Det torde krävas särskilda åtgärder för att säkerställa att den goda ordning som kännetecknar pappersbaserad diarieföring bibehålls även i IT-miljön.

Utformningen och användningen av adresser för elektronisk post rör alltså valet av infrastruktur på området. Planerna på en nationell teleadresskatalog ger ett angeläget tillfälle att genomlysa frågan.

Elektroniska akter, m.m.

1 Bakgrund

Vissa underförstådda och självklara rutiner för att skapa god ordning är knutna till den traditionella indelningen i olika mål och ärenden, där varje mål/ärende i sinnevärlden utgörs av pappershandlingar sammanhållna till en akt, med tillhörande dagboksblad eller motsvarande noteringar.[38] Handlingarna hålls vanligtvis ordnade kronologiskt, omslutna av en aktkappa, och kan överblickas med stöd av noteringarna på dagboksbladet. Sådan aktbildning är allmänt förekommande inom rättskipning och förvaltning, och även om vissa myndigheter har en annan ordning för vissa ärendekategorier, är aktläggning dock det normala sättet för arkivering.

Genom dessa rutiner, som fungerar väl i pappersmiljö, blir det enkelt att tillgodose parternas rätt att i en rättegång eller ett förvaltningsförfarande ta del av det myndigheten grundat sitt avgörande på, och vid ett överklagande får nästa instans del av allt processmaterial genom att akten sänds över.

Det finns ingen lagreglering rörande aktbildning, dagboksblad, etc. för domstolarnas eller förvaltningsmyndigheternas handläggning av mål eller ärenden enligt FPL eller FL. I RB föreskrivs emellertid att parternas inlagor och andra handlingar i ett mål eller ett ärende, samt rättens protokoll och avskrift av domen och sådant beslut som sätts upp särskilt, skall sammanföras till en akt, där också föreläggande eller andra beslut som inte har intagits i protokoll skall upptas genom anteckning på inlaga eller på annat sätt.[39] Vidare föreskrivs att dagbok skall föras över alla mål, som utvisar tiden då varje mål inkommit, vidtagna åtgärder, etc.[40]

Metoden att i en akt fixera vad som förekommit är svår att förena med användningen av register, där uppgifterna struktureras från andra utgångspunkter än i en traditionell skriftlig handling, vanligtvis med sikte på att möjliggöra en snabb sökning och presentation av uppgifter om ett visst objekt, t.ex. uppgifterna i bilregistret om en bil eller i fastighetsregistret om en fastighet. Det uppfattas inte som avgörande vem som svarar för en viss uppgift eller har begärt en viss åtgärd, eller vem som har beslutat eller annars genomfört en viss ändring i registret. Huvudsaken är att myndigheten ansvarar för att registret som helhet är korrekt.

[38] Jfr Wennergren, Handläggning, 15 u., s. 12.

[39] 6 kap. 10 och 12 §§ RB, se även 6 kap. 13 § RB och 16-21 §§ och 21 c § protokollskungörelsen (1971:1066).

[40] 6 kap. 11 § RB, jfr 14, 15, 21 a och 21 b §§ protokollskungörelsen.

Som exempel på denna skillnad mellan hanteringen av akter resp. egentliga register kan nämnas handläggningen av en ansökan om lagfart avseende fast egendom. Ärendet handläggs på grundval av ingivna pappershandlingar och en pappersutskrift av innehållet i fastighetsregistret rörande den aktuella fastigheten. Därvid bildas en akt med traditionella undertecknade pappershandlingar, och den som beslutar i ärendet signerar en utskrift som arkiveras, medan beslutet förs in i registret och expedieras till sökanden på papper, från Lantmäteriverket.

Den som vill granska ärendehandläggningen får alltså ta del av traditionellt material hos en inskrivningsmyndighet, medan den som är intresserad av aktuella uppgifter om fastigheten endast behöver ta del av det centralt förda registret.

Myndigheternas IT-rutiner är till stor del utformade på detta sätt, dvs. att den huvudsakliga handläggningen sker manuellt medan delrutiner har datoriserats, t.ex. hanteringen av uppgifter som behöver vara lätt åtkomliga för många.

2 Planerade rutiner

Utvecklingen går nu mot rutiner där även hanteringen av akter, dagboksblad, diarier etc. sker elektroniskt. På t.ex. skatteområdet har sådana rutiner redan lagreglerats, och det pågår eller planeras nya IT-baserade rutiner inom stora delar av förvaltningen. Domstolsverket bedriver också arbete på området. Det är emellertid oklart vilka tekniska, administrativa och rättsliga lösningar som bör väljas på olika områden, och behovet av vägledning är stort.

Som exempel på en tillämpning kan nämnas de nya rutinerna för elektronisk dokumenthantering inom skatteförvaltningen. Under det utredningsarbete som låg till grund för regleringen på skatteområdet skisserades följande modell för att rättsligt beskriva IT-användningen.[41]

När en kontrolluppgift som skall lämnas enligt skatteförfattningarna kommer in till en skattemyndighet, uppkommer ett ärende vid myndigheten. Uppgifterna kan lämnas på såväl papper som datamedium eller genom teleöverföring direkt till skattemyndighetens informationssystem. Pappersbaserade handlingar scannas.[42] Uppgifter kontrolleras maskinellt av skattemyndigheten beträffande rimlighet m.m., och materialet samlas i elektroniska akter.[43]

[41] Ds 1994:80 s. 77 f.

[42] Här finns visserligen mer teknikneutrala begrepp såsom bildfångst och imaging, men scanning är det som i praktiken har kommit att användas.

[43] Begreppet elektronisk akt används som beteckning på de handlingar som finns i ett ärende, både handlingar som har upprättats i elektronisk form och elektroniska avbildningar av pappershandlingar (prop. 1994/95:93 s. 26).

Kontrolluppgiften läggs i en elektronisk akt avseende uppgiftslämnandet, samtidigt som uppgifter om innehållen preliminärskatt enligt kontrolluppgiften tillförs resp. skattskyldigs elektroniska deklarationsakt för avstämningar mot uppgifter om inbetald preliminärskatt. De uppgifter som tas in i en skattskyldigs akt förs in i den blankett för förenklad deklaration som myndigheten sänder ut.[44] När deklarationen kommer in scannas den och tillförs den elektroniska deklarationsakten. Pappersdeklarationerna bevaras också — i den mån gallring inte får ske — men de tas fram endast om en handlings äkthet ifrågasätts eller om det annars krävs av utredningsskäl.

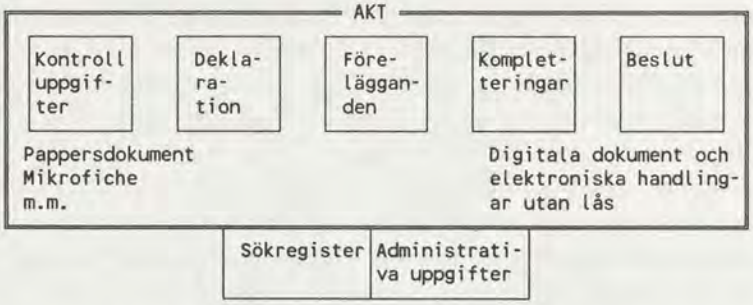
Vid ärendehandläggningen skall tjänstemannen med en ordbehandlingsfunktion kunna skriva föreläggande m.m., som tas in i den elektroniska akt som ärendet rör samt skrivs ut på papper och sänds till den skattskyldige. Elektronisk kommunikation utesluts dock inte, även om säkra rutiner för digitala signaturer m.m. saknas i ett enskilt fall, jfr kompletteringar per telefon. Pappersbaserade svarsskrifter och andra handlingar scannas och tas in i den elektroniska akten. Originalen arkiveras i den mån gallring inte får ske.

När ärendet är färdigt för avgörande sätts beslutet upp i elektronisk form och förses, vid automatiskt fattade beslut, med myndighetens digitala stämpel, och i övriga fall med handläggarens digitala signatur. Underrättelse om beslut avses vanligtvis ske genom utskrifter på papper. På sikt kan emellertid elektronisk kommunikation antas bli möjlig.

Det behövs också noteringar som underlag för åtkomst till elektroniska akter, samt möjlighet att notera och strukturera administrativa uppgifter, bl.a. för att ärenden skall kunna lottas på viss handläggare och att handläggare skall kunna göras uppmärksamma på nya handlingar som kommit in, en frist som löpt ut, etc. Rutiner behövs vidare för att skilja ut och gallra s.k. mellanprodukter, minnesanteckningar och andra elektroniska handlingar i den mån de inte behöver bevaras.

Den elektroniska deklarationsakten i det elektroniska förfarandet kan illustrerades med följande figur.

[44] Detta behöver vid modern datalagring, t.ex. i en relationsdatabas, inte innebära att en uppgift måste registreras två gånger. Avgörande är att den som tar del av en akt får fram aktuell handling.



I lagstiftningsärendet betonades att databehandlingens syfte är att stödja sådan ärendehandläggning där undertecknade pappershandlingar vanligtvis används. Dokument som skall överföras elektroniskt från en enskild till skatteförvaltningen eller vice versa, samt beslut och andra handlingar som upprättas och förvaras elektroniskt hos skatteförvaltningen, behöver därför skyddas så att det, på motsvarande sätt som vid en användning av pappersurkunder, kan prövas om ett dokument är äkta. Vidare behöver handlingarna struktureras så att ärendehandläggningen fungerar lika rättssäkert som i traditionell miljö.

Riksskatteverket har som målsättning att också självdeklarationen skall kunna ges in helt elektroniskt.[45] Kravet på informationssäkerhet avses uppnås bl.a. genom en användning av digitala signaturer och digitala stämplar.[46]

I sammanhanget berördes också förfarandet att elektroniskt avbilda (scanna) och IT-lagra inkomna pappershandlingar så att handläggarna kan ta del av uppgifterna på bildskärm. Detta jämfördes från rättslig utgångspunkt med rutiner där en myndighet grundar sin handläggning på fotokopior av skriftliga originalhandlingar.[47] Fotokopiorna vidimeras vanligtvis, och genom vidimeringen blir kopian att anse som urkund enligt 14 kap. 1 § andra stycket BrB. Den som vidimerar står som ett slags garant för handlingens bevisfunktion.[48] På motsvarande sätt kan digitala dokument upprättas genom bildteknik, t.ex. så att den som ansvarar för scanningen av ett visst dokument, till den elektroniska avbildningen knyter en signatur eller en stämpel av vilken framgår att

[45] Uppgifter om näringsverksamhet, som skall lämnas på blankett enligt fastställt formulär, får dock efter särskilt medgivande lämnas på ADB-medium. Det är emellertid inte fråga om något helt papperslöst deklarationsförfarande (19 § fjärde stycket lagen /1990:325/ om självdeklaration och kontrolluppgifter och prop. 1990/91:5 s. 87 f. och 121).

[46] Metoden att bereda skydd genom att en terminalanvändare måste bekräfta sin identitet genom ett hemligt *lösenord* kan visserligen rätt utformad binda en utställare till ett meddelande men en lösenordsmetod låser inte texten så att man kan veta att den är oförvanskad.

[47] En av myndighet vidimerad fotokopia har i vissa fall ansetts till och med kunna användas som fångeshandling vid ansökan om lagfart (prop. 1970:20 med förslag till jordabalk, del A s. 288 f. och 412).

[48] Beckman m.fl., Brottsbalken II, 6 u., s. 73.

den elektroniska bilden överensstämmer med det pappersbaserade originalet.[49] Enligt min mening krävs närmare överväganden om formerna för detta och vilka krav på säkerhet som bör ställas för sådana rutiner.[50]

3 Överväganden

3.1 Allmänt

Mitt uppdrag innefattar sådana rutiner där även hanteringen av akter avses ske elektroniskt. Det behöver därvid, såsom vid traditionell akthantering, kunna avgöras vem som har ställt ut en elektronisk handling i en elektronisk akt och vem som har vidtagit eller annars ansvarar för en åtgärd. Vidare behöver handlingarna i ett mål eller ett ärende kunna presenteras samlat. Handlingarna skall registreras[51], och deras ursprung och samband skall kunna visas så att de avspeglar handläggningsprocessen. Rätten till partsinsyn och offentlighetsinsyn skall också tillgodoses, i den mån ett utlämnande inte hindras av bestämmelser om sekretess,[52] och det skall i efterhand kunna utläsas vilka uppgifter som legat till grund för ett avgörande. Elektroniska akter bör således struktureras och bevaras så att de krav på god ordning och överblickbarhet, som ses som självklara i traditionell miljö, tillgodoses också i IT-miljön.

När dessa förutsättningar föreligger finns inga hinder från rättssäkerhetssynpunkt att införa elektronisk akthantering. I praktiken har det emellertid visat sig att datoriseringen ofta innefattar en sådan omdaning av verksamheter att processmaterial inte alltid kan presenteras samlat. Genom användningen av ny teknik har rutinerna blivit alltmer splittrade. Handlingarna i ett ärende kan vara fördelade på olika medier, och det förekommer att det inte finns något "arkivexemplar" av en handling utan att den får sammanställas ur myndighetens databas. Det har visat sig vara svårt att på detta sätt återskapa handlingar i efterhand. En anledning är att databaser i allmänhet uppdateras fortlöpande.[53] Detta gäller även när uppgifterna har avställts för bevarande.

[49] Man kan också tänka sig att åsätta myndighetens elektroniska stämpel, men det kan antas vara värdefullt att den som ansvarar för framställningen av avbildningen, vid behov, kan identifieras och höras om hur åtgärden gått till, t.ex. om det kontrollerats att förlagan varit undertecknad och alltså inte utgjordes av en fotokopia.

[50] Jfr. 3 kap. 6 § RA-FS 1994:2.

[51] Se vidare 15 kap. sekretesslagen.

[52] Se vidare 16 och 17 §§ FL, 43 § FPL, 2 kap. TF. och 14 kap. 5 § sekretesslagen.

[53] Enligt arkivlagen får en myndighet dock inte oreglerat radera i databaser som utgör allmänna handlingar. Innan ändringar görs i ADB-upptagningar som utgör allmänna handlingar skall ett bevarande av de ursprungliga uppgifterna säkerställas (4 kap. 4 § RA-FS 1994:2).

Det är således betydelsefullt att redan i handläggningsskedet säkerställa ett bevarande av just de uppgifter som legat till grund för handläggningen av ett mål eller ett ärende. Ett sådant krav följer av bl.a. 14 § DL där det föreskrivs att en myndighet, som för handläggning av mål eller ärende använder sig av en ADB-upptagning, skall tillföra upptagningen till handlingarna i målet eller ärendet i läsbar form, om inte särskilda omständigheter föranleder annat. Ett bevarande säkerställs också av 6 § arkivlagen där det föreskrivs att arkivet skall organiseras så att tillgången till allmänna handlingar underlättas. Vidare finns bestämmelser om registrering av handlingar i 15 kap. sekretesslagen.

Enligt min mening behövs inte på lagnivå någon ny reglering av myndigheternas akthantering.[54] En sådan reglering skulle tvärt om kunna begränsa eller rent av hindra utvecklingen av nya mera rationella rutiner. Det bör vara tillräckligt att det klargörs vad som avses med elektroniska handlingar och digitala dokument, och att dessa, med anknytande rutiner, sätts in i sitt rättsliga sammanhang, samtidigt som klara besked ges om vikten av god ordning och rättssäkra rutiner.[55] Därmed behöver allmänt accepterade betraktelsesätt rörande hanteringen av akter inte ändras annat än marginellt i IT-miljön.

De komplikationer som kan uppkomma torde ha samband med att processmaterialet, åtminstone under en avsevärd övergångsperiod, kommer att bevaras delvis elektroniskt, delvis på papper. Möjligheterna till strukturering och rationalisering med stöd av IT bör tas till vara, antingen så att det pappersbaserade materialet scannas[56] och tillförs den elektroniska akten, eller så att väl fungerande hänvisningar och rutiner för bevarande bidrar till att allt material i ett mål eller ärende enkelt kan presenteras samlat. Härvid bör rutinerna kunna göras begripliga genom analogier med traditionella rutiner. En akt hålls samman elektroniskt i stället för av en fysisk kappa, och dokumenten säkerställs med digital signatur eller digital stämpel i stället för en underskrift. Handläggaren bör, på motsvarande sätt som i en pappersakt, kunna "bläddra" i de elektroniska handlingar som hör till den elektroniska akten. Han bör vidare enkelt kunna skriva föreläggande, beslut och tjänsteanteckningar, signera dem och föra dem till respektive akt. Om visst processmaterial finns endast på papper bör det klart framgår att en

[54] Sådana regler finns dock i Riksarkivets författningssamling.

[55] Att denna praktiska syn på akthanteringen inte står i strid med den rättsliga regleringen framträder särskilt när det beaktas att vad som utgör en akt vid en domstol kan beröra mer än en "sak" och att många lagar — även sådana som knyter an till RB — har ett annat målbegrepp än RB, oftast ett begrepp som motsvarar RB:s rättegångsbegrepp. (Fitger m.fl. Rättegångsbalken I, s. 14:6, jfr Ds 1994:80 s. 159).

[56] Efter vidimering och signering bör en scannad avbildning av en pappersbaserad urkund kunna jämföras med en av myndighet vidimerad papperskopia av en urkund, förutsatt att rutinerna fått en lämplig utformning.

sådan handling finns i ärendet[57], jfr hur t.ex. ett tillhygge som ges in som bevis i ett brottmål noteras på det dagboksblad som hör till brottmålsakten (aktbilageras), men sedan i enlighet med gjorda noteringar förvaras på annan plats än i akten.[58]

Det är alltså ett minimikrav att handlingarna kan presenteras samlat i *läsbar* form, t.ex. på en bildskärm eller i form av utskrifter. I praktiken kan det emellertid ofta visa sig lämpligt att också i *lagrad* form förvara de handlingar som hör till ett visst ärende samlat.

I RB finns som framgått vissa bestämmelser om akthantering. Eftersom denna reglering inte hindrar elektroniska rutiner har jag inte funnit skäl att nu föreslå några författningsändringar på området.[59] I den mån det visar sig behövas närmare regler för elektronisk akthantering bör sådana föreskrifter kunna ges på lägre nivå. Riksarkivet har redan utfärdat vissa verkställighetsföreskrifter med anknytning till sådan akthantering, t.ex. angående förfarandet vid scanning.[60]

3.2 *Ytterligare funktioner för en säker akthantering*

På motsvarande sätt som behovet av informationssäkerhet m.m. tillgodoses genom användningen av digitala dokument och säkra rutiner för bevarande av handlingar, kan behovet av tillit till att samtliga handlingar finns med i en elektronisk akt och att alla anteckningar på ett elektroniskt dagboksblad finns kvar och är oförvanskade, tillgodoses genom digitala signaturer och digitala stämplar.

Ännu framstår dock sådana rutiner vanligtvis som alltför långtgående. Frågan bör bedömas från fall till fall. Höga krav på säkerhet kan behövas t.ex. i ärenden där mycket känsliga personuppgifter finns, där större penningbelopp hanteras eller när en elektronisk akt "lånas ut" till en annan myndighet.[61]

Här bör också nämnas de rutiner som används, med kuvert som klistrats igen med särskild tejp, för att skydda handlingar som har hemligstämplats (15 kap. 3 § första stycket sekretesslagen). Digitala signaturer med anknytande s.k. säkerhetstjänster (kryptering) kan användas också för att hindra olovlig insyn. Åtkomsten kan begränsas

[57] Prop. 1994/95:93.

[58] Jfr. 3 kap. 1 § RA-FS 1994:2, där krav ställs på att samband i arkivbildningen inte får brytas vid överföringar mellan olika medier.

[59] Uttrycken "avskrift" och "anteckning å inlaga" behöver inte heller tas upp i detta sammanhang.

[60] Se 3 kap. RA-FS 1994:2, jfr prop. 1994/95:93 s. 26.

[61] Jfr att domstolarna i vissa fall syr ihop akter. I IT-miljön sker dock inte "utlåning" så att själva arkivexemplaret lämnas ut. För att undvika t.ex. manipulationer framställs ett nytt elektroniskt exemplar som inte avses återlämnas, se vidare 5 kap. 9 § RA-FS 1994:2. I framtiden kommer "utlåning" troligtvis att ske så att data överförs via nät samtidigt som skyddet för uppgifterna knyts till själva data.

så att endast den som är behörig att handlägga frågan om utlämnande kan göra handlingen läsbar (jfr 15 kap. 3 § andra stycket sekretesslagen).

Det finns alltså tekniska möjligheter att elektroniskt hantera skyddet för sekretessbelagda elektroniska handlingar. Inte heller här krävs emellertid några särskilda lagregler för IT-miljön.

3.3 Särskilt om uppgifter som hämtas från register

Den som avgör ett mål eller ett ärende kan ha tagit del av uppgifter i ett register, t.ex. utdrag ur bilregistret vid handläggningen av ett ärende som rör ett fordon. Eftersom denna typ av register uppdateras kan det bli svårt att i efterhand fastställa registrets innehåll vid den aktuella tidpunkten. Till detta kommer de komplikationer som uppträder när handlingarna i ett visst ärende skall presenteras samlat och vissa uppgifter inte finns i akten.

Frågan uppmärksammades vid datalagens tillkomst. Med utgångspunkt från den då självklara förutsättningen att handlingarna i mål och ärenden bevaras skriftligt, föreskrevs i 14 § DL att en ADB-upptagning som används för handläggning av mål eller ärende, skall tillföras handlingarna i målet eller ärendet i läsbar form, om ej särskilda skäl föranleder annat. Syftet med bestämmelsen är enligt lagmotiven att det i efterhand skall vara möjligt att klargöra vilka uppgifter som hade betydelse för avgörandet, och det angavs vidare ofta vara en förutsättning för en fungerande partsinsyn att upptagningarna har överförts till läsbar form. De risker för bristande IT-rutiner som uppenbarligen låg till grund för bestämmelsen i 14 § DL är visserligen lika aktuella nu, men flera invändningar kan göras mot bestämmelsen och dess placering.

(1) Den kan sägas uppta självklarheter som inte bör föranleda någon reglering i lag.

(2) Bestämmelsen är inte teknikneutral, och det finns en risk att den leder till motsatsslut.[62] Naturligtvis bör en akt innehålla även uppgifter som har hämtats ur *manuella* register som regelbundet uppdateras. En sådan komplettering kan ske t.ex. genom att en kopia av ett registerkort fogas till akten.

(3) Om undantaget för "särskilda skäl" ges en snäv tolkning skulle bestämmelsen kunna föra med sig en omfattande pappershantering eller rent av hindra en övergång till elektronisk akthantering.

(4) Bestämmelsens tillämpningsområde och syfte ger anledning att ifrågasätta om den hör hemma i FL — och kanske även i FPL och RB

[62] Jfr LEXIT-rapporten s. 39.

— i stället för i DL. Å ena sidan avser bestämmelsen både personuppgifter och andra uppgifter i elektronisk form: Den är alltså, till skillnad från huvuddelen av bestämmelserna i DL, inte begränsad till personregister. Å andra sidan är bestämmelsen — till skillnad från DL i övrigt — tillämplig endast om den elektroniska handlingen används i mål eller ärende, en begränsning som knyter an till tillämpningsområdet för RB, FL och FPL. Motsvarande regel i 15 § FL, för uppgifter som en myndighet får på annat sätt än genom en handling, är dock begränsad till sådana ärenden som avser myndighetsutövning mot någon enskild.

(5) Bestämmelsen i 14 § DL hör enligt Datalagsutredningen mer hemma i sekretesslagen än i DL. Utredningen har därför föreslagit att bestämmelsen oförändrad förs över till 15 kap. sekretesslagen (1980:100) som en ny 14 §.[63]

(6) Enligt Arkivutredningen bör det vid en framtida översyn av området övervägas att flytta bestämmelserna i 15 kap. sekretesslagen om registrering och utlämnande av allmänna handlingar m.m. till arkivlagen.[64]

I praktiken har undantaget i 14 § DL för "särskilda skäl" tolkats så att omfattande undantag förekommer,[65] och det kan ifrågasättas om bestämmelsen verkligen behövs. I RB finns som framgått redan regler om aktbildning, och det kan framstå som främmande att där föra in en bestämmelse för handlingar som har viss form och som tagits fram på visst sätt.[66] Det är så självklart att elektroniska handlingar, som har tagits fram ur ett register för handläggningen av ett visst mål eller ärende, skall tillföras akten i målet/ärendet, att en bestämmelse med sådant innehåll som sagt kan locka till felaktiga motsatsslut.[67] För den händelse handlingsbegreppet i t.ex. 6 kap. 10 § RB inte skulle anses innefatta elektroniska handlingar krävs andra åtgärder. På motsvarande sätt finns det skäl att ifrågasätta en sådan särbestämmelse för förvaltningsdomstolar och förvaltningsmyndigheter.

[63] SOU 1993:10 s. 468.

[64] SOU 1988:11 s. 192.

[65] Som exempel kan nämnas att regeringen vid införandet av elektronisk dokumenthantering inom skatteförvaltningen har tolkat undantaget så att inget hindrar att upptagningar tillförs en elektronisk akt i stället för en pappersbaserad akt, när akterna blir åtkomliga för part via bildskärm eller utskrift. Bestämmelsen hindrar därmed inte de rutiner för elektronisk akthantering som jag föreslår, där akterna skall vara lätt åtkomliga och uppfylla kraven rörande partsinsyn m.m., bl.a. genom att uppgifter som inhämtas från register tillförs akten (prop. 1994/95:93 s. 34, jfr Ds 1994:80 s. 138 f.).

[66] En regel som den i 14 § DL skulle i anknytning till RB närmast framstå som en upprepning av den föreskrift som redan finns om att handlingarna i ett mål skall sammanföras till en akt (6 kap. 10 § RB).

[67] Jfr den kritik som framfördes mot Datastraffrättsutredningens förslag att i 35 kap. 4 § RB föra in en erinran om behovet av att beakta risker för fel i samband med automatisk informationsbehandling.

Enligt min mening är den naturliga lösningen att bestämmelsen helt upphävs såsom varande överflödig. Med hänsyn till att man på många håll hyser farhågor för att ett upphävande av bestämmelsen skulle medföra en ökande risk för bristfälliga rutiner och till att bestämmelsen inte hindrar att elektroniska rutiner införs lägger jag emellertid inte fram något formellt förslag i denna del. Ett upphävande bör kombineras med en betydande informationsinsats till alla berörda myndigheter.

Förvaltningslagen och IT

1 Allmänt

De grundläggande reglerna i förvaltningslagen (1986:223; FL) för förvaltningsmyndigheternas formella behandling av ärenden gäller oberoende av om ärendehandläggningen sker manuellt eller med stöd av IT och bestämmelserna är allmänt hållna. Vid en övergång till säkra rutiner för signerade elektroniska handlingar behövs därför vanligtvis inga regler som direkt avviker från de synsätt som ligger bakom FL. Visserligen för de planerade rutinerna med sig nya förutsättningar för den förvaltningsrättsliga regleringen men det har i samband med tull- och skattedatoriseringen visat sig att elektronisk ärendehandläggning vid manuellt beslutsfattande och datoriserad signering fordrar endast marginella avsteg från regleringen av traditionella rutiner. Avvikelser från FL bör alltså endast undantagsvis komma i fråga.

I det följande behandlar jag de frågor rörande FL som bör kommenteras med avseende på elektronisk dokumenthantering.[68] Härvid aktualiseras frågor om bl.a. anhängiggörande, muntlig handläggning, partsinsyn, kommunikation, beslutsmotivering och underrättelse om beslut samt rättelse av beslut och bekräftelse av meddelanden som inte har undertecknats. Slutligen berörs vissa anknytande frågor, bl.a. om användning av vissa begrepp och om det tekniska förfarandet.

2 Elektroniskt anhängiggörande, m.m.

Myndigheternas verksamhet innefattar inte bara administrativt handlande, som främst tar sig uttryck i ärendebehandling, utan även s.k. faktiskt handlande. Med handläggning av ett ärende brukar normalt avses hela den procedur som börjar med ett ärendes anhängiggörande och slutar med dess avgörande.

Gränsen mellan ärendehandläggning respektive annat administrativt eller faktiskt handlande är emellertid flytande.[69] I IT-miljön kompliceras denna fråga av att åtgärder på alla nivåer kan vidtas mer eller mindre automatiskt med hjälp av datorer, samtidigt som behovet av teknisk expertis har lett till att t.ex. telebefordrings- och dataserviceföretag får i uppdrag att sköta vissa uppgifter, bl.a. i samband med överföringen av handlingar till en myndighet. Härvid kan bl.a. frågor om när ett ärende skall anses anhängiggjort och huruvida en åtgärd är att anse som ärendehandläggning bli oklara.

[68] Jfr Cecilia Magnusson Sjöberg, Rättsautomation, 1992, s. 307 f.

[69] I gränsfall måste på grundval av en ändamålsbestämning avgöras om en företeelse verkligen utgör handläggning av ärenden i förvaltningslagens mening (Wennergren, Handläggning, 15 u., s. 13 f.).

När ett ärende anhängiggörs utifrån brukar det inte vara några svårigheter att avgöra vid vilken tidpunkt ärendet uppstår. Ärendet blir anhängigt när den handling som aktualiserar ärendet har kommit in till myndigheten i enlighet med de bestämmelser om elektroniskt inkommande som jag föreslår (förslagen till 33 kap. 3 a § RB, 44 a § FPL och 10 a § FL).[70] Tidpunkten för anhängiggörande är svårare att bestämma när ärendet initieras av myndigheten.

Efter det att en handling — på ingivarens risk — har befordrats till myndighetens elektroniska adress, och ett ärende därmed har blivit anhängigt, är det emellertid i IT-miljön vanligt att handlingen — på myndighetens risk — skall befordras t.ex inom myndighetens nät till ett lokalkontor eller från en elektronisk myndighetsadress hos ett befordringsföretag till myndighetens informationssystem. Ärendet prövas först därefter i sak.[71]

Myndigheterna behöver härvid vara uppmärksamma på hur rutinerna för befordran m.m. utformas så att datoriserade kontroller eller andra ingrepp, t.ex. när tekniska fel uppkommer, inte oavsiktligt ges sådan ingripande utformning att myndighetsutövning äger rum på ett stadium där detta inte är avsett. Vanligtvis förvaras och databehandlas befordrade elektroniska handlingar endast som ett led i överföringen, och det är inte meningen att någon skall vidta åtgärder så att en handläggning av ett visst ärende påbörjas. Det är emellertid en trend att på ett så tidigt stadium som möjligt införa olika kontrollrutiner, i vissa fall på dokumentnivå, och att anlita t.ex. dataservice- eller telebefordringsföretag för dessa uppgifter. Om denna förvaltningsuppgift innebär myndighetsutövning[72] får den emellertid inte utan stöd i lag överlämnas till en juridisk person eller en enskild individ.[73]

Mina förslag till reglering av inkommande handlingar innebär att också en elektronisk handling som inte kan läsas av myndigheten är att anse som inkommen. Detta aktualiserar vissa praktiska frågor. Enligt min mening bör handlingar, som myndigheten inte kan läsas eller på grund av tekniska fel annars inte kan använda, få återtas i huvudsak formlöst, jfr det formlösa återtagande som är vedertaget beträffande inskrivningsärenden där handlingarna återsänds efter en anteckning i

[70] Jfr TDL-utredningens syn på anhängiggörande när elektroniska dokument nått tullens mottagningsfunktion (SOU 1989:20 s. 155 f.).

[71] Det föreligger dock inget hinder mot att påbörja beredningen av ett ärende så snart handlingarna är tillgängliga och har registrerats, se t.ex. TDL-utredningens jämförelse med ett inskrivningsärende enligt jordabalken. Om en ansökan inkommit mellan två inskrivningsdagar anses den gjord på den senare, något som inte hindrar att ärendena bereds för avgörande så snart handlingarna blir tillgängliga. En inskrivningsmyndighet måste naturligtvis vid sin ärendehandläggning iaktta gällande regler för förfarandet oavsett om inskrivningsdagen inträtt eller inte.

[72] Ang. detta begrepp, se t.ex. Hellners/Malmqvist, Nya Förvaltningslagen, 4 u., s. 150 f. och Lena Marcusson, Offentlig förvaltning utanför myndighetsområdet, s. 171 f.

[73] 11 kap. 6 § tredje stycket RF, jfr prop. 1994/95:93 s. 37 f.

dagboken. Det bör härvid inte krävas något formellt beslut om avskrivning, om en myndighet av tekniska skäl stoppar en elektronisk handling och enligt rutiner som görs upp med ingivaren återsänder eller annars avför handlingen i avvaktan på nytt material. Myndigheterna bör inte heller belastas med lagringen av sådana elektroniska handlingar som inte avses användas, om bevarandet saknar betydelse från rättssäkerhetssynpunkt. Regleringen av en sådan gallring bör kunna ske i förordning eller på lägre nivå. Här krävs emellertid vaksamhet så att det praktiska förfarandet inte leder till att en frist blir försutten.

Genom det beskrivna synsättet anknyter hanteringen av elektroniska handlingar och akter på ett naturligt sätt till de pappersbaserade rutinerna. De behov som kan visa sig föreligga att alltjämt basera handläggningen av vissa ärenden på pappersurkunder kan därmed naturligt knytas till IT-rutinerna.

3 Muntlig handläggning och anteckning av uppgifter

Den elektroniska akthanteringen bör utformas så att parterna kan lämna uppgifter muntligt och få dem antecknade i akten, om det kan ske med hänsyn till arbetets behöriga gång. Därmed behövs inte någon regel som avviker från 14 och 15 §§ FL.

Frågan om att enligt 14 § DL tillföra akten uppgifter som en handläggare har tagit del av i ett register har behandlats i *bilaga 6* under rubriken "Särskilt om uppgifter som hämtas från register".

4 Partsinsyn

Enligt 16 § FL har en sökande, klagande eller annan part rätt att ta del av det som har tillförts ärendet, om detta avser myndighetsutövning mot någon enskild. För dessa fall har frågan om sekretess reglerats i 14 kap. 5 § sekretesslagen (1980:100).

De elektroniska akterna med digitala dokument, elektroniska dagboksblad och liknande noteringar skall naturligtvis utformas så att FL:s regler om partsinsyn kan tillämpas även i den nya miljön. Det får härvid bedömas från fall till fall om handlingarna skall presenteras på bildskärm eller på papper. Därmed behövs ingen särskild reglering för IT.

5 Kommunikation och beslutsmotivering

Det är väsentligt att den elektroniska akthanteringen ges en sådan utformning att också principerna om kommunikation, beslutsmotivering och underrättelse om beslut inte sätts ur spel. Rutinerna måste utformas så att hittillsvarande praxis enligt 17 § FL kan upprätthållas, om nya

uppgifter från en utomstående tillförs en elektronisk akt. Myndigheten skall då, vanligtvis elektroniskt eller via pappershandlingar, underrätta sökanden och ge denne tillfälle att yttra sig om det inte är obehövligt.

Enligt 20 § FL skall ett beslut, med vissa undantag, innehålla beslutsmotivering. Den föreslagna användningen av digitala dokument och akter medför att motiveringar skall kunna skrivas in och förvaras elektroniskt på motsvarande sätt som i pappersmiljö. Det är betydelsefullt att myndigheterna när IT-rutiner införs, liksom beträffande indelningen av materialet i akter, noggrant går igenom vilka rutiner för beslutsstöd m.m. som bör gälla, så att de krav som följer av bestämmelserna om beslutsmotivering uppfylls.

6 Rättelse av beslut

Enligt 26 § FL kan en myndighet rätta ett beslut som till följd av skrivfel, räknefel eller något annat sådant förbiseende innehåller en uppenbar oriktighet. Beträffande IT-baserade beslutsdokument bör sådana rättelser kunna utformas på ett sätt som är parallellt med rättelse av pappersdokument. Om man föredrar att rätta "i" det digitala dokumentet kan rättelserutinen tekniskt utformas så att den nya texten signeras tillsammans med den ursprungliga, och presenteras i läsbar form som om användaren hade tillfört rättelsen på samma underlag. Härvid får naturligtvis inte det ursprungliga digitala dokumentets innehåll ändras. Även när rättelsen sker på ett sätt som för användaren inte ser ut så att rättelse sker "i" det ursprungliga dokumentet bör det nya dokumentet med rättelsen naturligtvis signeras. Vidare bör anknytande tekniska och administrativa uppgifter kompletteras så att det, för den som skall ta del av akten, klart framgår att en rättelse har ägt rum.

Statens offentliga utredningar 1996

Kronologisk förteckning

1. Den nya gymnasieskolan - hur går det? U.
2. Samverkansmönster i svensk forsknings-finansiering. U.
3. Fritid i förändring. Om kön och fördelning av fritidsresurser. C.
4. Vem bestämmer vad? EU:s interna spelregler inför regeringskonferensen 1996. UD.
5. Politikområden under lupp. Frågor om EU:s första pelare inför regeringskonferensen 1996. UD.
6. Ett år med EU. Svenska statstjänstemäns erfarenheter av arbetet i EU. UD.
7. Av vitalt intresse. EU:s utrikes- och säkerhetspolitik inför regeringskonferensen. UD.
8. Batterierna - en laddad fråga. M.
9. Om järnvägens trafikledning m.m. K.
10. Forskning för vår vardag. C.
11. EU-mopeden. Ålders- och behörighetskrav för två- och trehjuliga motorfordon. K.
12. Kommuner och landsting med betalnings-svårigheter. Fi.
13. Offentlig djurskyddstillsyn. Jo.
14. Budgetlag - regeringens befogenheter på finansmaktens område. Fi.
15. Union för både öst och väst. Politiska, rättsliga och ekonomiska aspekter av EU:s sjätte utvidgning. UD.
16. Förankring och rättigheter. Om folkomröstningar, utträdesrätt, medborgarskap och mänskliga rättigheter i EU. UD.
17. Bättre trafik med väginformatik. K.
18. Totalförsvarspliktiga m95. Förslag om jobb/studier efter muck, bostadsbidrag, dagpenning, försäkringar. Fö.
19. Sverige, EU och framtiden. EU 96-kommitténs bedömningar inför regeringskonferensen 1996. UD.
20. Samordnad rollfördelning inom teknisk forskning. U.
21. Reform och förändring. Organisation och verksamhet vid universitet och högskolor efter 1993 års universitets- och högskolereform. U.
22. Inflytande på riktigt - Om elevers rätt till inflytande, delaktighet och ansvar. U.
23. Kartläggning och analys av den offentliga sektorns upphandling av varor och tjänster med miljöpåverkan. N.
24. Från Maastricht till Turin. Bakgrund och övriga EU-länders förslag och debatt inför regeringskonferensen 1996. UD.
25. Från massmedia till multimedia - att digitalisera svensk television. Ku.
26. Ny kurs i trafikpolitiken + Bilagor. K.
27. En strategi för kunskapslyft och livslångt lärande. U.
28. Det forskningspolitiska landskapet i Norden på 1990-talet. U.
29. Forskning och Pengar. U.
30. Borgenärsbrotten - en översyn av 11 kap. brottsbalken. Fi.
31. Attityder och lagstiftning i samverkan + bilagedel. C.
32. Möss och människor. Exempel på bra IT-användning bland barn och ungdomar. SB.
33. Banverkets myndighetsroll m.m. K.
34. Aktiv arbetsmarknadspolitik + expertbilaga. A.
35. Kriminalunderrättelseregister DNA-register. Ju.
36. Högskola i Malmö. U.
37. Sveriges medverkan i FN:s familjeår. S.
38. Nationalstadsparker. M.
39. Rapport från klimatdelegationen 1995. Klimatrelaterad forskning. M.
40. Elektronisk dokumenthantering. Ju.

Statens offentliga utredningar 1996

Systematisk förteckning

Statsrådsberedningen

Möss och människor. Exempel på bra IT-användning bland barn och ungdomar. [32]

Justitiedepartementet

Kriminalunderrättelseregister
DNA-register. [35]
Elektronisk dokumenthantering. [40]

Utrikesdepartementet

Vem bestämmer vad? EU:s interna spelregler inför regeringskonferensen 1996. [4]
Politikområden under lupp. Frågor om EU:s första pelare inför regeringskonferensen 1996. [5]
Ett år med EU. Svenska statstjänstemäns erfarenheter av arbetet i EU. [6]
Av vitalt intresse. EU:s utrikes- och säkerhetspolitik inför regeringskonferensen. [7]
Union för både öst och väst. Politiska, rättsliga och ekonomiska aspekter av EU:s sjätte utvidgning. [15]
Förankring och rättigheter. Om folkomröstningar, utträdesrätt, medborgarskap och mänskliga rättigheter i EU. [16]
Sverige, EU och framtiden. EU 96-kommitténs bedömningar inför regeringskonferensen 1996. [19]
Från Maastricht till Turin. Bakgrund och övriga EU-länders förslag och debatt inför regeringskonferensen 1996. [24]

Försvarsdepartementet

Totalförsvarspliktiga m95. Förslag om jobb/studier efter muck, bostadsbidrag, dagpenning, försäkringar. [18]

Socialdepartementet

Sveriges medverkan i FN:s familjeår. [37]

Kommunikationsdepartementet

Om järnvägens trafikledning m.m. [9]
EU-mopeden. Ålders- och behörighetskrav för två- och trehjuliga motorfordon. [11]
Bättre trafik med väginformatik. [17]
Ny kurs i trafikpolitiken + Bilagor. [26]
Banverkets myndighetsroll m.m. [33]

Finansdepartementet

Kommuner och landsting med betalningssvårigheter. [12]
Budgetlag - regeringens befogenheter på finansmaktens område. [14]
Borgenärsbrotten - en översyn av 11 kap. brottsbalken. [30]

Utbildningsdepartementet

Den nya gymnasieskolan - hur går det? [1]
Samverkansmönster i svensk forskningsfinansiering. [2]
Samordnad rollfördelning inom teknisk forskning. [20]
Reform och förändring. Organisation och verksamhet vid universitet och högskolor efter 1993 års universitets- och högskolereform. [21]
Inflytande på riktigt - Om elevers rätt till inflytande, delaktighet och ansvar. [22]
En strategi för kunskapslyft och livslångt lärande. [27]
Det forskningspolitiska landskapet i Norden på 1990-talet. [28]
Forskning och Pengar. [29]
Högskola i Malmö. [36]

Jordbruksdepartementet

Offentlig djurskyddstillsyn. [13]

Arbetsmarknadsdepartementet

Aktiv arbetsmarknadspolitik + expertbilaga. [34]

Kulturdepartementet

Från massmedia till multimedia - att digitalisera svensk television. [25]

Näringsdepartementet

Kartläggning och analys av den offentliga sektorns upphandling av varor och tjänster med miljöpåverkan. [23]

Civildepartementet

Fritid i förändring.
Om kön och fördelning av fritidsresurser. [3]
Forskning för vår vardag. [10]
Attityder och lagstiftning i samverkan + bilagedel. [31]

Miljödepartementet

Batterierna - en laddad fråga. [8]
Nationalstadsparker. [38]
Rapport från klimatdelegationen 1995. Klimatrelaterad forskning. [39]

KUNGL. BIBLIOTEKET STOCKHOLM

FRITZES
Postadress: 10647 Stockholm
Fax 08-205021, Telefon 08-69090 90