Dag Wiese Schartum og Anne Gunn B. Bekken (red.)

YULEX 2009

Senter for rettsinformatikk / Avdeling for forvaltningsinformatikk
Postboks 6706 St Olavs plass
0130 Oslo

Henvendelser om denne bok kan gjøres til:

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

ISBN 978-82-7226-123-7
ISSN 0806-1912

Utgitt i samarbeid med Unipub
Trykk: AIT e-dit AS
Omslagsdesign Kitty Ensby

Kjære leser,

Her er en liten julehilsen fra alle ansatte ved Senter for rettsinformatikk og Avdeling for forvaltningsinformatikk.

Når vi nå snart tar farvel med 2009 kan vi se tilbake på en rekke høydepunkter. Vi begynte året med internasjonal konferanse i Oslo om Internet Governance, med tilhørende bokutgivelse på Oxford University Press. I januar ble også Personvernkommisjonens innstilling overlevert - ikke minst takket være iherdig innsats fra flere personer i vårt miljø. Dette var også året da vi lanserte tjenesten Personvernskolen.no, og gjorde avtale med to departementer om å utvikle IT-støtte for lov- og forskriftsarbeid. I tillegg kan jeg nevne to dagers eForvaltningskonferanse, to dagers Nordisk konferanse i rettsinformatikk om «Overvåking i en rettsstat», og avslutning av året med Personvernkonferansen 2009. Også undervisningsaktiviteten er omfattende med ansvar for bl.a. to masterprogrammer og et bachelorprogram. Jeg tror derfor det er lett å si seg enig i at også 2009 har vært et aktivt år!

Størst av alt for et forskningssenter er når phd-arbeider får en lykkelig slutt. I år har vi hatt gleden av én disputas og i tillegg vil tre stipendiater ha levert avhandlingene sine til bedømmelse før året er slutt. Tidlig neste år vil ytterligere to av våre stipendiater levere avhandling innen det rettsinformatiske fagområdet. Er det rart vi er stolte og glade?!

I 2010 fyller SERI 40 år, og vi kan med stor tilfredshet registrere at jubilanten holder koken på alle måter. Vi avslutter året med femten ansatte og ti tilknyttede forskere, og regner med å være minst like mange til neste år. Limet i virksomheten er vår lille men aktive administrasjon som sørger for at alt går på skinner til tross for bred aktivitet og høyt tempo.

Jeg håper denne lille uhøytidelige samlingen av artikler vil være til glede, og gi deg lyst til å holde kontakten med oss ved Senter for rettsinformatikk og Avdeling for forvaltningsinformatikk også til neste år. Forhåpentligvis ses vi på noen av våre konferanser og seminarer, eller vi kan ha gleden av forskningssamarbeid. Men først skal vi feire jul og hvile godt ut!

God jul og godt nytt år!

Dag Wiese Schartum
(senterleder)

Dear Reader,

This is a little Christmas greeting from all of the staff members at the Norwegian Research Center for Computers and Law and the Section for eGovernment Studies.

As we approach the close of 2009, we are able to look back on a series of high points. We began the year with an international conference in Oslo on Internet Governance, with a concurrent publication at Oxford University Press. January also marked the issuance of the Data Protection Commission's recommendations - in no small degree due to the energetic efforts of several persons in our academic community. This was also the year we launched Personvernskolen.no [Data Protection School] and entered into agreements with two departments for the development of IT support for work in the areas of statutes and regulations. In addition I might mention the two-day eGovernment conference, the two-day Nordic Conference in Legal Informatics covering the topic «Surveillance in a Legal State», and the end-of-year 2009 Data Protection Conference. Teaching activity has also been comprehensive, including responsibility among other things for two master programs and one bachelor program. In view of all of this, I think it is easy to agree that 2009 has been a very active year!

The crowning achievement for any research center is when PhD work is successfully concluded. This year we have had the pleasure of acknowledging the successful presentation of one thesis; in addition three research fellows will have submitted their theses for evaluation before the end of the calendar year. In the early months of next year, two more of our research fellows will submit their theses in the field of legal informatics. Is it any wonder, then, that we are proud and happy about these achievements?!

In 2010 SERI will celebrate its 40th anniversary, and we are understandably pleased to note that the center remains viable and active in every way possible. We close the current year with a staff of fifteen, along with ten associate researchers, and we expect to have just as many personnel during the coming year. Coordinating our activity are the members of our small but very active administration, who see to it that things run smoothly and productively despite a broad range of activities and a hectic work pace.

I sincerely hope that this informal compendium of articles will be a source of inspiration and will encourage you to stay in touch with us at the Norwegian Research Center for Computers and Law and the Section for eGovernment Studies in the coming year. Hopefully we will see you at some of our conferences and seminars, and perhaps we can have the pleasure of cooperating on

certain research topics. Before we do that, however, we plan to celebrate the Christmas holidays and enjoy a much deserved respite!

Merry Christmas and a Happy New Year!

Dag Wiese Schartum
Director of the Center

CONTENTS

THE FUTURE OF THE TRADE IN INFORMATION – AND A WORLD HISTORY OF THE LEGAL TYPES OF CONTRACTS GIVING ACCESS TO INFORMATION[1]

Jon Bing

Introduction: The trade in Information

It is unusual to be invited to speculate over the possible development of the law. My own interest in information systems and intellectual property law has been a basis for an interest in considering the legal framework for a trade in «information» or «knowledge». These terms are not in this paper used in a technical sense – for instance qualifying the difference between «information» (semantics), «data» (syntactic) and «signs» (atomic), perhaps with «knowledge» as a pragmatic fourth member. I will use the terms in an informal way, hoping the context will be sufficient for the reader to understand the meaning. In this way, «information» will include many different aspects: The advice of a lawyer or a consulting engineer to a client will be an example of «information», as will the reports of a news service, a science fiction novel or a rock opera.

When considering the future, it is often useful to look back and consider the development up to the present – it is like an archer drawing the string of his bow back in order to give the arrow impetus to plunge forwards to the target.

1 A brief history of the trade in information: From the beginning to the present

The *first* example of trade in information might have happened in the Stone Age. One hunter approaches another and offer advice: He knows where there is a valley in which fat bison graze. He is willing to reveal the location of this

1 Paper presented at the Conference *«The future of…Conference of Law and Technology»* 28-29 October 2008, Florence, Italy. Under publication.

valley for a fee, for instance a royalty of one bison ham for each animal actually killed by the other.

This might be the first example of a consultancy contract. It has one important condition – the existence of a spoken language which makes it possible for the consultant to peddle his advice to the hunter. And it has two critical limitations – the unity of time and place. The transaction has to take place with both persons present at the same time and at the same location; they have to be within earshot of each other.

The payment has to be agreed before the information actually is exchanged. The «administration of rights» is limited to choosing *not* to communicate if the terms are not satisfactory. After the communication, there is no practical way to control the use of the knowledge as such apart from brute force (for instance banging the hunter in the head with a club if the royalty is not paid as agreed), and there is the risk of the hunter communicating the information to a third party without informing the original consultant or including him or her in the transaction.

This may be an example of the first trades in information, but it is still very popular. Not only is there still consultants around, but employment contracts are generally based on the presumption that the employee can contribute through his or her experience, knowledge or insight to the business of the employer. It is the knowledge of the employee that most often is the reason for hiring or contracting a person rather than this person's strong arms or beautiful face.

The *second* example presumes that writing has been invented, that is a system of written signs which can communicate information. This occurred approximately two thousand years BC, almost simultaneously in Sumer and Egypt – probably somewhat later in the Indus valley. In Sumer, the information was represented by cuneiform characters made by pressing a wooden triangular tool in a wet clay tablet. Luckily some of these tablets was fired, and have therefore been preserved. In Egypt, hieroglyphs were carved in stone or painted on walls. Writing originally was motivated for accounting purposes. The cities developing in the Middle East required a trade in agricultural products with the surrounding districts, and the writing was necessary to keep track of purchases and payments. But the writing made it possible to record more interesting information, like the *Epic of Gilgamesh*. The story is probably the first example of fiction, not claiming to be am myth or legend of the past or gods. It is a variant of the Perseus myth: The King of Babylon determines by oracle that his grandson Gilgamesh will kill him, and throws him out of a high tower. An eagle breaks his fall, and the infant is found and raised by

a gardener. The epic was retrieved in 1853 when excavating the library of the last great Assyrian king, Ashurbanipal (1200 BC).

Writing made it possible to imprint signs on physical objects – like clay tablets, rolls of papyri, books of vellum or paper. The object was subject to trade like any other objects – it could be purchased or sold, if there was a market for such objects, the imprinted signs being a property of the object like an elaborate carving or a polished surface. The fact that the value was related to the information communicated by the text rather than the function of the object was not very important in a legal perspective. The object was a *unicum*.

The writing broke the unity of time and place. The information could be communicated over time (as our own reading of the tablets with the story of Gilgamesh demonstrates). A favorite example of mine[2] is what happened when the Caliph of Bagdad, Nasir, decideds to ask Djengis Khan for assistance against his enemy, Shah Mohammed. Making sure the written request does not fall into the hands of the Shah, the Caliph has the head of one of his slaves shaved, then tattoos the message on the scalp, and waits for the hair to grow out and cover the text. The he sends the slave through the enemy lines until he finds the Khan, who shaves the head of the slave once more to read the request. The Khan refuses to help the Caliph, and that is the end of the story – which does not tell us what happened to the slave after his career as a data carrier was brought to an end.

In this context, the law of the sales of goods sufficed. The «administration of rights» was limited to the control of the physical carrier. No further elaboration was necessary.

But this was changed, of course, when Gutenberg invented the printing process 1448.[3] Prior to his invention, it has been estimated that there were 30 000 volumes of books in Europe. Fifty years later – approximately 1500 – there were three hundred printing shops in Venice alone, and the number of books had increased to 15 million![4] The impact on society was major, but we look towards the impact on law.

It is rather obvious that the old form of «rights management» no longer was sufficient. Printers were in competition. A printer could identify an interesting text in Greek or Latin; have it translated into Italian and experience great demand, selling a large number of copies. However, the printer next

2 Tor Åge Bringsværd: *Gobi: Min prins*, Gyldendal, Oslo 1994:208.

3 Printing from moveable type was actually invented in Korea prior to Gutenberg, the oldest printed book being the *Buljo Jikji*.(1372). But the invention of printing in Korea did not have the socio-political consequences that Gutenberg's invention had in Europe.

4 Sources give rather different figures, though the relative relation remains the same. The text is based on Helmer Dahl *Teknikk, kultur, samfunn,* Ingeniørforlaget, Oslo 1982:33.

door thought it unreasonable that only his neighbor should enjoy success, so copied the text and sold his own reproductions – to a lower price, because he did not have to pay a translator. To regulate the market, the Venetian republic resorted to the traditional solution of the middle ages: The republic awarded a «patent», that means an exclusive right to a printer to reproduce a certain text or book. Originally this was a right awarded the printer, but occasionally the privilege was given also to the author. One of the early examples was Ludevico Ariosto, the author of one of the more famous novels of the Italian renaissance, *Orlando furioso,* which first appeared in 1515. This tells about Roland, one the paladins of Charlemagne and misfortune in losing his wits, which he luckily can retrieve by travelling to the Moon.[5]

The Venetian solution was exported, for instance to England where the Stationary Guild, organising the printers, kept a record of which of its members had been granted an exclusive right to reproduce which texts. This record was known as a register of «copy rights».

This is indeed a sketchy indication of one of the origins of the modern copyright. But it may suffice to demonstrate how it was developed in order to meet the challenge of the dev elopement of information technology. Before the printing press, possession was sufficient to govern the rights to the text in a book. But this was not sufficient for the printer – and the notion of an «intellectual right» was born, a right to reproduce the text residing in the text as an abstract object, today we call this a «work».[6]

This system of rights management has been carried onwards to modern times. According to the conventional publisher's contract, the author authorises the reproduction of an edition (the number of copies being specified). The printer confirms this with a receipt from the printing, and the publisher furnishes an annual statement of how many copies have been sold. Typically the author has a right to inspect the warehouse to ascertain the number of copies in store. In such a way, the author is supervising that his or her right to payment in the form of royalty (a fraction of the price paid for a copy by the end user) is fulfilled.

Similar schemes were developed and implemented for other types of physical objects carrying information – like phonograms, videos *etc*. They all were

5 In the wall of Albergo del Sol (which may be the oldest hostel in the world) at Piazza del colonna in front of the Pantheon in Rome, there is a plaque stating that Ludevico Ariosto stayed there in March through April 1513.

6 There are another important basis, clearly stated by the decision of the French parliament of 15 March 1586 to award the rights of the French poet and scientist Marc-Antoine Muret to his heirs, each person being the owner of what he or she had created as God governs what he has created.

based on control of the objects, the stock. But there were alternative schemes for rights management developed – for instance – for the public performance of music or dramatic works, the broadcasting of works *etc*. In most cases this was based on contractual agreements between the producer (theatre) or broadcaster, which was possible in practice because there were rather few of them. This was not possible for public performance of music, and for the administration of the rights of authors (the composer, the writer of lyrics *etc*), a system of collective societies developed, each authorised by the individual copyright holder to represent them, and with reciprocal international agreements to represent the portfolio of rights held by sister organisations.

Until the 20th century information could only be traded in these two categories – either as a service or employment contract with the person who had the information (experience, skill or whatever) in his or her head, or by purchasing a physical object in which the information was recorded in a certain script. Certainly there may be examples that do not fit into the very general categories characterised above, but they will just be details in the general design. There is no claim made that this grossly simplified outline is appropriate for any purpose, it is just drawn to emphasise the typical characteristics of the development in the trade in information.

2 The invisible copies

The third category of trade was made possible by information technology. Today we are comfortable in selling the *representation* – the signs, the characters – separately from a physical medium, and certainly without involving an individual's real time services. This is what we do when we download a file, send an email, and browse the Internet *etc*. It is part of our daily routines. But when it first emerged, it was perceived as something new – at least by those who were able to cast the technological development in legal terms, like Michael Keplinger[7] in his paper «The Case of the invisible copies».[8] It is mainly related to computers and the fact that any representation of information may be computerised: Text in the form of codes identifying the sign of a script represented, sound in the form of sampling the frequencies at very short intervals and representing the frequency as a number, and pictures by resolving an image into tiny squares (pixels) and entering codes for the blend of colours (red, blue, green) and gray scale for each pixel.

7 Mr Keplinger is currently Deputy Director General of the World Intellectual Property Organization (WIPO) in the Copyright and Related Rights and Enforcement Sector.

8 *Revue International de Droit d'Auteur*, October 1970

This make it possible to trade in information without there being (1) human beings communicating within the unity of time and space, or (2)) without any physical object changing hands. This is a new way of trading information. This simple observation has several consequences.

One is that the other two categories of trade are associated with major changes in the history of man. The spoken language is by many seen as the characteristic setting man apart from animals. And the written language is closely related to the development of the cities in the Middle East, which at least formed the foundation of the European culture.

Second is that the traditional schemes for the administration of rights fail. There is no «consultant» to make communication of information conditional to a fee, as in our Stone Age example. And there is no physical object which can be controlled to ensure payment of royalty or similar remuneration for making the object available (like selling a painting).

Some has in this failure of the traditional schemes for the administration of rights seen the failure of copyright as such – that is the failure of the original Venetian strategy of a right in an abstract object, the copyrighted «work».

Obviously this is too facile. In the information society, there is an even greater importance than before placed on the need to exchange information, and to take sufficient payment for information. Information technology makes information more important. Therefore there is a need for a legal regime for govern the trade in information. Indeed, we are in a situation not too unlike the aftermath of the Gutenberg invention. The old ways for the administration of rights to information fail due to the novel reproduction technology. There is a need to govern the market in order for it to develop and give society the advantages promised by the technology. Therefore there has to be found an alternative to the traditional way for the administration of the rights.

3 Digital Rights Management

There has been suggested that the answer to the challenge of the computerised systems is Digital Rights Management (DRM), and the WIPO Copyright Treaty of 1996 Art 11 introduces an obligation to members to «provide adequate legal protection and effective legal remedies against the circumvention of effective technological measures that are used by authors in connection with the exercise of their rights».

But the technical solutions for DRM have been rather primitive. They have mainly taken the form of access control (also conditional access control deployed for cable or satellite television), perhaps best known as the encryption

schemes protecting movies on a DVD.[9] Or the solution has been a copy control, made controversial by the inclusion of compact disk carrying music, and to a large extent abandoned by phonogram producers as a protection strategy. In my opinion, these attempts of introducing DRM systems have been too crude to be general, and have therefore generated bad-will with the policy backfiring into the more general legal development. However, it would be wrong to interpret this as a general failure of DRM. It should rather be interpreted that DRM has to meet certain requirements in order to win user acceptance, and obviously will have to be more sophisticated than what is exemplified above.

An example may be a scenario developed by Giovanni Sartor and myself.[10] There is no need to repeat the scenario in all its details, but the three basic elements can be emphasised:

First, the work to be purchased has to be *identified*. The purchaser may know something about the work, typically author, performing artists, title or even a digital object identifier (DOI)[11] or similar identifier. For music, the purchaser may not know much at all, but sampling the music, an electronic fingerprint can be formed and used as a key to access one of the several existing public available databases, identifying not only the work, but also the exact session from which this performance of the work has been recorded. In this way, the purchaser has many ways to identify the work he or she wants to have made available.

Second, the DRM will be flexible, and will interact with software for the management of licenses residing on the end user's computer or digital device. This implies that the end user may purchase a license tailor-made to the desired use. If the work is a song, the licence will determine whether the song should be available for one time performance, or for a longer period, or even permanent, whether the licence should permit reproduction or only access, for private or public performance, *etc*. Such diversity obviously presumes the presence of an infrastructure not yet available. But it would make it possible for the end user to purchase a licence designed for the user he or she want to make

9 The Norwegian prosecution of «DVD-Jon», a teenager who posted a descrambling program for circumventing the access control of DVDs, has become well known. DVD-Jon was aquitted. The decision is available in English translation at several websites, see for instance http://www.ictlex.net/?p=61 (the translation is by the author).

10 The scenario is presented in several versions, but is generally known as the «Lovely Rita Scenario», after the song «Lovely Rita Meter Maid» by Lennon and McCartney, which is the subject for trade in the example, see for instance Jon Bing and Giovanni Sartor «Lovely Rita: A Scenario» in Jon Bing and Giovanni Sartor (eds) *The Law of Electronic Agents*, CompLex 4/03, Norwegian Research Center for Computers and Law, Oslo 2003:11-21.

11 Cf http://www.doi.org/.

of the work, and it will relate to the payment. This in contrast to the «one seize suits all»-DRM solutions we have seen up till now.

Third, the complexity indicated above has to be set off by smarter consumer technology. This would make it extremely simple to purchase works on the net. In the scenario, it is suggested that the solution is developed using autonomous intelligent electronic agents – computer programs that have sufficient knowledge based technology components to make them able to negotiate on behalf of the end user. The agents of the end user would negotiate with agents of the right holders, offers would be compared and the agents would try to make the best bargain, guided by instructions given by the end user.

Therefore, behind the scenes there would be a greater complexity than today. There would be a large choice of different licences interacting with monitoring software on the device of the end user. There would be negotiations by electronic agents, perhaps hundreds of parallel negotiations going on before the «best buy» would be qualified. But in front of the stage would be the simple world of the end user – the consumer listen to a tune, perhaps on an old-fashioned radio broadcast and pushes the button «purchase». His or her agent flings itself into cyberspace, carrying with it the pre-instructions of its owner, identifying the tune, accessing possible alternative sources, negotiating price and licensing terms with the agents representing the right holders, initiating payment from the end user's account at the same time as the music file is made available to the end user for the device or devices the end user will prefer for accessing the file and enjoying the music. And the music will be available for the end user before the music has been played to its end by the broadcast. A purchase made simple by complex technology.

Regrettably the payment scheme necessary for such a scenario is not fully developed. But the ease of purchase will – it is suggested – ensure trade, and the variety of licenses will ensure freedom of choice.

Of course the payment will be one of the crucial elements. iPod has demonstrated that the end user is willing to pay if the purchase scheme is simple and user friendly, and also the price not unreasonable. In the future market there will be a large variety of pricing schemes in parallel. The pricing will vary between phonogram producers (the «big four» dominating the current international stage), YouTube videos uploaded by individuals, advertisements, academics posting their own papers, self-promotion of different kinds, *etc*. A similar variety will be in the licensing terms, and the terms will be enforced by programs residing within the device of the end user (or, if this is a «thin» device, as possibly will become more common, the programs will govern the end user access point to the net).

The simple or brute solutions of the past have proved too brittle to be sustained over time. They will possibly be replaced by a variety of technically more complex solutions, ensuring free consumer choice. This profusion of possibilities may at first glance be mistaken for a confusion – but there is an important difference been confusion and profusion. Information of different kinds – text, images and sound – will be available by many very different services, and also there will be many solutions. But they will have one thing in common – they are easy to use, otherwise they will not will end user acceptance.

And for the consumer, it all will be perceived as simple and easy. The end user may not understand the complexity behind the scenes – in the same way that a person in front of a television screen hardly understand the technology bringing him or her the high definition movie that he or she is enjoying. That does not overly bother the consumer, for the end user it is simple – a touch to a button on the remote control. Like the «one-click purchase» of amazon.com tomorrow's information services for the consumer will be models of simplicity – on the surface.

4 A final word

It may be fitting to end this little essay on the future of the trade in information by an example of a work of fiction, which in our future may be subject to such trade. It also may offer some comfort to those who feel that the issues are too many and too complex really to grasp, and feel overwhelmed by the policy issues brought to us on the foaming crests of the waves of the onrushing future. It an aphorism by the Norwegian author Gene Dalby:[12]

«He, who holds his head above the waters,
sees only the tip of the iceberg.»

12 From his collection *Den tatoverte tungen (The tattooed tongu),* Aschehoug, Oslo 1986. Translation by the author.

KAN OPPHAVSRETTEN LÆRE NOE FRA DEN TINGSRETTSLIGE ALLEMANNSRETTEN NÅR DET GJELDER UTFORMING OG FORSTÅELSE AV DE OPPHAVSRETTSLIGE LÅNEREGLER? [1]

Thomas Rieber-Mohn

1. Innledning

1.1 Tema

Tingsretten og opphavsretten utgjør to separate og forskjellige «rettighetsuniverser», og det har ikke vært spesielt vanlig å trekke inn argumenter fra tingsrettslig tenkning ved utforming av opphavsrettslige regler. Tvert imot vil nok ofte den grunnleggende forskjellen mellom tingsrett og immaterialrett tilsi at det søkes *forskjellige* løsninger i de to relasjonene. Overgangen til et digitalt samfunn har imidlertid vist seg å være en stor utfordring for opphavsretten, og til tross for en rekke lovgivertiltak og intense debatter i teorien de siste tiårene strever man fortsatt med å finne et godt «grep» for å balansere rettighetshaverens og samfunnets interesser i denne sammenheng.[2] Dette kan tyde på at tradisjonelle opphavsrettslige løsninger kommer til kort i den digitale kontekst, og at det der er behov for *nye*. I denne artikkelen undersøkes om tingsretten her kan bidra med noe, nærmere bestemt om opphavsretten har noe å lære av den tingsrettslige *allemannsretten* når det gjelder utforming og forståelse av de opphavsrettslige låneregler.

---

1 Artikkelen er en bearbeidet versjon av prøveforelesningen forfatteren holdt over oppgitt emne i tilknytning til sin doktordisputas ved Det juridiske fakultet, Universitetet i Oslo den 21. august 2009. Forfatteren arbeider i dag som advokat ved Kluges avdeling for IKT og immaterialrett.

2 Forfatterens egen doktoravhandling, «Digital privatkopiering – åndsverkloven § 12 i møte med tekniske beskyttelsessystemer og rettslige omgåelsesforbud» (foreløpig upublisert) kan ses som et tegn på at jakten på en tilfredsstillende løsning i denne sammenheng ennå ikke er avsluttet.

1.2 Definisjoner

Den tingsrettslige allemannsretten kan vi med *Falkanger* definere slik:

> *«I motsetning til i mange andre land har allmennheten hos oss fra gammelt av kunnet utøve en viss bruk over annen manns eiendom – den være seg eiet av private eller av staten. Samlebegrepet for denne tillatte bruk er allemannsretten.»* [3]

Et sentralt trekk ved allemannsretten er altså at den *avgrenser eierens rådighet over fast eiendom* – han må finne seg i at eiendommen brukes av enhver innefor allemannsrettens rammer. Eieren kan ikke i kraft av sin eiendomsrett motsette seg slik bruk.

Opphavsrettens låneregler innebærer på sin side at visse typer bruk av åndsverk kan utøves *uten opphavsrettshaverens samtykke*, selv om bruken egentlig faller inn under de opphavsrettslige eneretter, slik de er definert i åndsverkloven § 2. Et sentralt trekk ved lånereglene er altså at de avgrenser opphavsrettshaverens rådighet over verket: Selv om vi er innenfor hans definerte eneretter, kan han ikke i kraft av opphavsretten motsette seg slik bruk som lånereglene utpeker. Vi aner vel allerede en slags parallellitet mellom de to regelverkene.

1.3 Nærmere om problemstillingen

Opphavsrettens utfordringer i digital sammenheng skyldes først og fremst det som er blitt kalt «det digitale dilemma»[4]: På den ene siden er det med digital teknologi blitt vesentlig enklere å kopiere og distribuere opphavsrettsbeskyttet innhold, og risikoen for rettighetsbrudd er derved økt betraktelig. På den annen side muliggjør teknologien tilnærmet fullstendig *kontroll* med tilgang til og bruk av digitalt innhold. I forhold til lånereglene er det særlig denne siste siden av dilemmaet som skaper problemer: Faren er at rettighetshavere ved bruk av såkalt DRM[5]-teknologi vil «stenge inne» innholdet på en måte som uthuler opphavsrettslige brukerfriheter.

Problemene med å finne en løsning ut fra tradisjonell *opphavsrettslig* tenkning, tvinger opphavsrettsjuristen til å løfte blikket. Det blir relevant å søke

---

3 Thor Falkanger, *Fast eiendoms rettsforhold*, Oslo 2007 s. 168. Av pedagogiske hensyn kan det kanskje være grunn til å presisere at allemannsretten er noe annet enn *allmenning*sretten i norsk tingsrett. Det er *allemanns*retten – og ikke allmenningsretten – som er temaet her.

4 Uttrykket ble brukt av den amerikanske Committee on Intellectual Property Rights and the Emerging Information Infrastructure, som i 2000 fremla sin rapport «The Digital Dilemma: Intellectual Property in the Information Age».

5 Digital Rights Management.

etter inspirasjon og eksempler utenfor det opphavsrettslige – endog utenfor det immaterialrettslige – univers. Med en slik åpen tilnærming kan det være nærliggende å rette fokus mot den tingsrettslige allemannsretten: Som antydet, har allemannsretten og låneregelene *det klare fellestrekk* at begge kan sies å representere en «beskjæring» av bestående private rettigheter, basert på krysssende samfunnshensyn.

Artikkelens problemstilling forutsetter en komparativ analyse av allemannsretten og opphavsrettens låneregler. Det er to forhold som skal sammenlignes: reglenes *utforming* og *forståelsen* av dem. Med «utforming» forstår jeg i denne sammenheng hvordan *lovgiver* har utformet reglene. «Forståelse» tolker jeg som en henvisning til hvordan reglene er blitt oppfattet og anvendt i det praktiske rettsliv, først og fremst i rettspraksis og juridisk teori. Hvordan skal en så bedømme *om* opphavsretten har noe å lære? Læring forutsetter for det første at noe *kan* gjøres annerledes. Et første skritt er derfor å undersøke om det foreligger *forskjeller* mellom de to regelsettene. Bygger allemannsretten på andre tilnærminger eller løsninger enn låneregelene? Hvis slike forskjeller eksisterer, blir neste spørsmål om allemannsrettens løsninger *bør* anvendes *også i opphavsrettslig sammenheng*. Noe forenklet må målestokken må her være om det «er noe å hente» for opphavsretten ved å annektere allemannsrettens løsninger: Kan man med det oppnå et alt i alt bedre *opphavsrettslig* regelverk.

1.4 Avgrensninger

Allemannsretten er en skandinavisk rettskonstruksjon, og tilsvarende regler finnes både i Sverige og Finland.[6] Likevel har jeg funnet det formålstjenlig å avgrense *min* analyse til allemannsretten i norsk rett. Det skyldes at den norske allemannsretten i alt vesentlig er lovfestet. Både den svenske og den finske allemannsretten har, til sammenlikning, fortsatt et primært sedvanerettslig grunnlag. De lovfestede norske reglene danner etter min vurdering et vesentlig bedre utgangspunkt for den analysen jeg skal foreta, der bl.a. reglenes *utforming* er et hovedtema. Jeg avgrenser derfor som nevnt til den *norske* allemannsretten.

For *låneregelene* er det ikke behov for en like stringent avgrensning til norsk rett. Idealet om *nordisk rettsenhet* står sentralt på opphavsrettens område, og alle de nordiske landene har regler som mer eller mindre tilsvarer de norske låneregelene. De konklusjoner jeg trekker vil derfor i stor grad også ha relevans for de øvrige nordiske lands opphavsrett. Ved gjennomgangen vil jeg likevel, for oversiktens skyld, ta utgangspunkt i den norske loven. Derimot er

6 For svensk retts vedkommende; se Åsa Åslund, *Allemansrätten och marknyttjande*, Linkøping 2008. Se også Gunnar Zettersten, *Allemansrätten i Norden*, København 1997.

det grunn til å trekke et skille mot mer åpne og skjønnsbaserte opphavsrettslige avgrensningsregler, slik som for eksempel den amerikanske «fair use»-doktrinen. For slike åpne standarder er det ikke sikkert at en sammenlikning med allemannsretten vil være like fruktbar. Uansett er det ikke vanlig å omtale denne typen avgrensningsregler som «låneregler». Jeg vil derfor avgrense mot slike mer åpne regler og standarder.

1.5 Opplegg / disposisjon

Jeg skal først, under pkt. 2, gi en komparativ fremstilling av de to regelsettene. Siden jeg dukker inn i materien fra et opphavsrettslig ståsted, vil det bli brukt mest tid på å beskrive de tingsrettslige reglene. Samtidig vil jeg peke på korresponderende opphavsrettslige regler – i den grad slike eksisterer. Deretter, under pkt 3, skal jeg drøfte om det ligger noen *lærdom* å hente her for opphavsretten.

2 Komparativ fremstilling – utforming og forståelse

2.1 Rettighetsstruktur

a Allemannsretten

Allemannsretten utgjør som nevnt inngrep i eiendomsretten. Norsk rett bygger i dag på et *funksjonelt* eiendomsrettsbegrep, som innebærer at eieren har all den rettslige og faktiske rådighet *som ikke positivt er unntatt* ved lov, avtale eller annen rettstiftende kjensgjerning.[7] Eiendomsretten er altså *negativt* avgrenset. Allemannsretten er i dette perspektivet *en* – eller rettere sagt en gruppe – av de rådighetsformene som positivt er unntatt fra eierens kontroll. Slik sett kan en kanskje si at allemannsretten er et ledd i den *praktiske* definisjonen av eiendomsretten.

b Låneregelene

Opphavsretten har et annet prinsipielt utgangspunkt enn eiendomsretten, idet opphavsrettshaverens enerett er *positivt* definert. Opphavsrettshaveren er i åndsverkloven § 2 gitt *to* beføyelser: eksemplarfremstilling og tilgjengeliggjøring for allmennheten. Det er disse to beføyelsene som definerer eneretten, og bruksmåter som faller utenfor er fri for enhver. Lånereglene har sitt virkefelt *innenfor* de to enerettsbeføyelsene og medfører at visse eksemplarfremstillings-

7 Falkanger, op.cit, s.38.

handlinger og visse tilgjengeliggjøringshandlinger *likevel* faller utenfor opphavsrettshaverens kontroll. Et annet strukturelt særtrekk ved lånereglene er at de kun gjelder verk som er *offentliggjort* eller *utgitt*. De har altså en grunnleggende *tidsmessig* begrensning ved at de ikke gjelder før opphavsmannen første gang gjør verket tilgjengelig for allmennheten.

2.2 Rettsgrunnlag, begrunnelse, subjekt og materielt innhold

a Allemannsretten

Som i Sverige og Finland, bygger den norske allemannsretten historisk sett på sedvanerett. I dag er den imidlertid lovfestet, og da hovedsakelig i friluftsloven av 1959. Også i vannressursloven § 16 og i straffeloven § 400 finner vi regler som det er naturlig å plassere under denne paraplyen, og dessuten sporadisk i enkelte andre lover. For oversiktens skyld vil jeg ved *min* gjennomgang hovedsakelig fokusere på friluftsloven – der vi finner de klart viktigste og klart fleste reglene om allemannsrett.

Allemannsretten kan historisk og kulturelt begrunnes i at det har vært et praktisk behov for å kunne benytte annen manns grunn på denne måten: Det er med andre ord ikke tilfeldig at slik bruk er blitt sedvane. På et mer prinsipielt plan kan dette underbygges med at allemannsretten gir en hensiktsmessig utnyttelse av fast eiendom. Dette er i bunn og grunn et *rettsøkonomisk* argument, som fremhever at et system *med* allemannsrett gir den mest effektive utnyttelsen av samfunnets ressurser. Som jeg skal komme tilbake til har etter hvert også friluftsinteressen – borgernes interesse i et aktivt og variert friluftsliv – fått en sentral og selvstendig posisjon i allemannsrettens begrunnelse. Det har m.a.o. vært en utvikling i det rettspolitiske fundamentet for allemannsretten, fra å være en nyttebasert nødvendig rett, til også å verne om den mer «unyttige» friluftsinteressen. Dette har skjedd parallelt med at den generelle samfunnsutviklingen har gitt borgerne stadig bedre tid og muligheter til å dyrke slike friluftsinteresser.

Allemannsretten gjelder enhver person. Alle kan utøve allemannsrett, også utlendinger som oppholder seg i Norge. Allemannsretten er en sammensatt gruppe bruksretter. Grovt sett kan den inndeles i tre: ferdsels-, oppholds- og høstingsretter. Slike rettigheter eksisterer, med noe varierende innhold, både på landjorden, i vassdrag og i sjø. Etter friluftsloven § 2 har man for eksempel rett til å ferdes i utmark hele året; § 6 gir rett til fri ferdsel med båt i sjø; § 7 en rett til landsetting og fortøyning av båt; § 8 en rett til bading og § 9 en rett til rasting og telting. Straffeloven § 400 gir rett til å høste nøtter, bær og andre naturforekomster på såkalt «uinnhegnet Sted». Dette for å nevne noen eksempler.

Friluftsloven opererer dessuten med et grunnleggende skille mellom *innmark* og *utmark*. Lovgiver har benyttet dette skillet som et grunnleggende verktøy i avveiningen mellom eierens og allmennhetens interesser:[8] Over *innmark* gjelder allemannsretten kun i sterkt begrenset utstrekning. Tolkningen og forståelsen av disse to kriteriene har derfor avgjørende betydning for allemannsrettens praktiske utstrekning. Rent systematisk er utmark *negativt* definert som «all udyrket mark som ikke er innmark».[9] Innmark er på sin side *positivt* definert i friluftsloven § 1a første ledd.

b Lånereglene

De opphavsrettslige lånereglene er lovfestet og er i norsk rett samlet i åndsverklovens annet kapittel. Hvis en ser på lånereglene enkeltvis, kan begrunnelsen sies å variere. Til illustrasjon er det primært hensynet til en *fri offentlig debatt* som begrunner *sitatregelen* i § 22, mens adgangen til eksemplarfremstilling til bruk *for funksjonshemmede* i § 17 er begrunnet i *de særlige behov* denne brukergruppen har. Fellesnevneren er imidlertid at lånereglene ivaretar ulike *samfunnshensyn*, som tilsier en avgrensning av de opphavsrettslige eneretter. Samtidig er lånereglene et viktig ledd i det mer overordnede opphavsrettslige regnestykket: En av opphavsrettens hovedfunksjoner er å stimulere til økt produksjon og distribusjon av åndsverk i samfunnet. *Det* kan – etter rådende oppfatning – best kan oppnås gjennom en *balanse* mellom eneretter og fri bruk – den såkalte «opphavsrettsbalansen». Lånereglene står helt sentralt i denne balanseringsoperasjonen.

Lånereglene kan ikke nødvendigvis påberopes av enhver. Derimot fremgår det av hver enkelt låneregel hvem subjektet er. Åndsverkloven § 13 gjelder for eksempel *lærere og elever*, mens § 23a gjelder *aviser, tidsskrifter og kringkasting*. Samlet sett dekker lånereglene en nokså mangeartet gruppe brukssituasjoner. Felles for dem alle er at de på nærmere vilkår åpner for enten *eksemplarfremstilling* eller *tilgjengeliggjøring for allmennheten* – det vil si handlinger som egentlig er forbeholdt opphavsrettshaveren.

8 Se Falkanger, op.cit., s. 169: «Lovgiveren har især foretatt avveiningen ved bruk av kriteriene innmark og utmark som defineres i friluftsl. § 1 a, og som tillegges betydning i §§ 2-4 og 7-9.»

9 Friluftsloven § 1a annet ledd.

2.3 System for håndtering av konflikter mellom eier- og brukerinteresser

a Allemannsretten

Med friluftsloven av 1959 fikk man også et administrativt system for håndtering av konflikter mellom allemannsretten og eiendomsretten. Disser reglene finnes i lovens annet kapittel. Loven tilbyr her et kobbel av virkemidler som kan tas i bruk for å avverge eller avdempe konflikter. Brukeren pålegges for eksempel plikt til å opptre hensynsfullt, og eieren har en viss adgang til å bortvise personer som ikke opptrer hensynsfullt.[10] Brukeren kan pålegges å betale erstatning for skade eller ulempe som voldes under utøvelse av allemannsrett.[11] Det gjelder et forbud mot såkalte «sjikanøse stengsler» for utøvelsen av allemannsrett.[12] Eieren har en viss mulighet til å innføre avgift for adgang til visse områder,[13] og til å innføre adferdsregler som brukeren må overholde.[14] I visse tilfeller kan områder sperres for allmennheten,[15] og eieren kan kreve at kommunen innløser en særlig utsatt tomt.[16] Dessuten kan en i tvilstilfelle innhente uttalelse fra kommunen, for eksempel i spørsmålet om et konkret område skal regnes som innmark eller utmark.[17]

Man kan i denne sammenheng også trekke frem friluftslovens *formålsbestemmelse*, selv om den kan sies å virke på et mer indirekte plan. Bestemmelsen er inntatt i § 1 og lyder slik:

> *«Formålet med denne loven er å verne friluftslivets naturgrunnlag og sikre almenhetens rett til ferdsel, opphold m.v. i naturen, slik at muligheten til å utøve friluftsliv som en helsefremmende, trivselskapende og miljøvennlig fritidsaktivitet bevares og fremmes.»*

Formålsbestemmelsen ble inntatt i loven i 1996 og er i forarbeidene begrunnet i «et ønske om å få nedfelt i loven de viktige og grunnleggende prinsipper for friluftslivet i Norge».[18] Det ble lagt vekt på at bestemmelsen skulle ha en «offensiv og framtidsrettet ordlyd», og under lovgivningsprosessen ble derfor ordet «fremmes» inntatt på slutten av bestemmelsen, i tillegg til «bevares».

10 Friluftsloven § 11.
11 Friluftsloven § 12.
12 Friluftsloven § 13.
13 Friluftsloven § 14.
14 Friluftsloven § 15.
15 Friluftsloven § 16.
16 Friluftsloven § 18.
17 Friluftsloven § 20.
18 Ot.prp. nr. 27 (1995-96), s. 15-16.

Som jeg skal komme tilbake, har formålsbestemmelsen stått sentralt for måten Høyesterett i ettertid har tolket og anvendt friluftslovens bestemmelser.

Friluftsloven gir på den annen side *ikke* vern mot at grunneieren endrer sin bruk av grunnen, f.eks. slik at det som tidligere var utmark blir til innmark. I tråd med det jeg har sagt, vil en slik bruksendring bety en drastisk innskrenkning av allmennhetens rett over den aktuelle grunnen. At friluftsloven likevel ikke gir noe vern mot slik faktisk omdisponering fra eierens side, er bl.a. stadfestet av Høyesterett i Rt. 2007 s. 102 (Ullrichsen), der det blant annet uttales at:

> *«Fortsatt er det nok slik at allmennheten, med forbehold for sjikanetilfellene, ikke på privatrettslig grunnlag kan motsette seg at grunneieren tar et område i bruk på en måte som hindrer utøvelsen av allemannsrettene.»*[19]

Her vil imidlertid andre lover komme til, som kan sikre at friluftsinteressen likevel blir ivaretatt. Dels er endringer i bruken av fast eiendom betinget av myndighetenes godkjenning, gjennom planlovgivningen. Ved behandlingen av søknader om slik godkjenning kan myndighetene hegne om allemannsretten, for eksempel ved at et samtykke til bruksendring tilknyttes vilkår om at allemannsretten respekteres eller vernes. Dels er i lov det lagt absolutte restriksjoner på eierens utnyttelse av grunnen. Det helt sentrale eksempelet i denne sammenheng er strandlovens generelle forbud mot bygging i 100-metersbeltet langs kysten.[20] Dette forbudet har som konsekvens at strandsonen i stor utstrekning *forblir* utmark, i friluftslovens forstand, og at allemannsretten derfor kan utøves der.

b Lånereglene

Åndsverkloven har tradisjonelt ikke hatt noe eget konflikthåndteringssystem á la det vi finner i friluftsloven. Det nærmeste man kommer er at loven, gjennom de såkalte tvangs- og avtalelisensene, har sikret rettighetshaveren et *rimelig vederlag* under enkelte av lånereglene.[21] Loven har i tillegg regler som pålegger brukere å opptre respektfullt i sin omgang med verket,[22] og den hjemler dessuten straff og erstatning ved rettighetsbrudd.[23] Derimot har den tra-

19 Rt. 2007 s. 102, avsnitt 74.
20 Plan og bygningsloven (1985) §17-2 første ledd / plan og bygningsloven (2008) § 1-8.
21 Det er vanlig å inndele lånereglene inn i tre grupper, nærmere bestemt fribruksregler, tvangs- og avtalelisenser, hvorav begge de to sistnevnte typer blant annet kjennetegnes ved at brukeren må betale for bruken.
22 Åndsverkloven § 11 jf. § 3.
23 Åndsverkloven kap. 7.

disjonelt ikke hjemlet særlige *tiltak* for å hindre skadelig bruk av åndsverk. Opphavsrettshaveren har for eksempel ikke noen lovfestet *bortvisningsrett* tilsvarende eierens rett etter friluftsloven § 11. I den grad det har oppstått konflikter, har partene vært henvist til å bringe dem inn for de ordinære domstoler.

Det er grunn til å fremheve at rettighetshaveren tradisjonelt heller ikke har hatt noen *praktisk* mulighet for å styre bruken av åndsverk: Så lenge verkseksemplar har vært gjort tilgjengelig, har besitteren av eksemplaret rent faktisk kunnet bruke det som han ville. I digital sammenheng er dette dramatisk endret. Ved bruk av DRM-teknologi kan rettighetshavere i prinsippet styre bruken av åndsverk ned til minste detalj – også etter at verkseksemplaret er overgitt til brukeren: På tilsvarende måte som grunneieren kan sette opp et gjerde, kan opphavsrettshaveren nå «gjerde inn» digitalt innhold med tekniske sperrer. Dette gir selvsagt også en mulighet for å blokkere slik bruk som lånereglene tillater. Lovgiver har både nasjonalt og internasjonalt tatt konsekvensen av denne utviklingen. I forbindelse med at åndsverkloven i 2005 fikk et generelt forbud mot omgåelse av DRM-teknologi,[24] ble det samtidig etablert en mekanisme for å beskytte de opphavsrettslige lånereglene. Omgåelsesreglene har bakgrunn i EUs opphavsrettsdirektiv,[25] og selve konflikthåndteringsmekanismen er inntatt i åndsverkloven § 53b:

> *«Rettighetshaver skal påse at den som har lovlig tilgang til et vernet verk, uten hinder av effektive tekniske beskyttelsessystemer kan gjøre bruk av verket, herunder fremstille nye eksemplarer, i henhold til §§ 13a, 15, 16, 17, 17a, 21, 26-28 og 31.*
>
> *Dersom rettighetshaver etter begjæring fra berettiget etter bestemmelsene ovenfor ikke gir tilgang som nevnt i første ledd, kan han etter begjæring fra den berettigede pålegges å gi slike opplysninger eller annen bistand som er nødvendig for å muliggjøre bruk av verket i samsvar med formålet. Begjæring rettes til nemnd opprettet av departementet etter regler som Kongen gir. Nemnda kan i tillegg til pålegg som nevnt, bestemme at berettiget etter nevnte bestemmelser uten hinder av § 53a kan omgå anvendte tekniske beskyttelsessystemer dersom rettighetshaver ikke overholder den frist nemnda setter for å etterkomme pålegget. …» (Mine uth.)*

Jeg skal ikke gå inn på detaljene her, men man kan med et kjapt blikk legge merke til at rettighetshaveren *pålegges å respektere* visse bestemte låneregler, og at brukeren blant annet gis en mulighet for å *klage* til en spesialoppnevnt

24 Åndsverkloven § 53a.

25 Europaparlaments- og rådsdirektiv 2001/29/EF om harmonisering av visse aspekter vedrørende opphavsrett og nærstående rettigheter i informasjonssamfunnet.

nemnd, hvis denne plikten ikke overholdes. Det er imidlertid en generell oppfatning at denne mekanismen er *utilstrekkelig*, dels fordi den ikke dekker *alle* lånereglene, dels fordi den er gjennomhullet av nokså omfattende unntak. Som jeg har antydet, mener derfor de fleste at det er behov for ytterligere tiltak dersom lånereglene skal sikres gjennomslag i en digital kontekst.[26]

2.4 Forståelsen av rettsposisjonene i teori og praksis

a Allemannsretten

Forståelsen av allemannsrettens natur har undergått klar utvikling de siste par hundre år. På 1800-tallet gikk det vi i dag omtaler som allemannsrett under betegnelsen «den uskyldige nyttesrett».[27] Betegnelsen peker i retning av at bruken måtte være både *nyttig* og *uskyldig*, for å være lovlig. Etter den alminnelige oppfatning hadde allmennheten heller ikke noen adgang til å håndheve denne rettsposisjonen.[28] Utover 1900-tallet ble imidlertid stadig mer vanlig i rettslitteraturen å benytte betegnelsen «allemannsrett». Et tidlig eksempel er Per Ryghs artikkel i TfR 1910, s. 255, der forfatteren konstaterte at det kan gjøres inngrep i såkalte «allemannsretter» uten at ekspropriasjon er påkrevd. I dag er det imidlertid ingen tvil om at allemannsretten er en *rett* i juridisk forstand – spørsmålet er mer *hvilken type* rett det er snakk om. Ut fra det foreliggende rettskildematerialet kan man imidlertid nokså sikkert slå fast følgende: Allemannsretten er en rettighet i den forstand at *enhver* kan håndheve den, for eksempel ved å anlegge sak for domstolene.[29] Samtidig står ikke allemannsretten like sterkt som en tingsrettslig særrett. I de aller fleste situasjoner vil den for eksempel savne ekspropriasjonsrettslig vern.[30]

Et *tredje* aspekt ved allemannsrettene er blitt fremhevet gjennom serie Høyesterettsdommer det siste tiåret: Rt. 1998 s. 1164 (Furumoa), Rt. 2005 s. 805 (Hvaler), Rt. 2007 s. 102 (Ullrichsen) og Rt. 2008 s. 803 (Collett). Disse dommene har først og fremst understreket allemannsrettens *dynamiske* karakter – at rettens innhold og utstrekning ikke er gitt en gang for alle. Dommene

26 Se f.eks. Thomas Rieber-Mohn, «Kravet til opphavsrettslig relevans som 'grunnsten' i det norske forbudet mot omgåelse av tekniske beskyttelsessystemer», *NIR* 4/2006, s. 321-335, med videre henvisninger.

27 Thor Falkanger, «Allemannsrett: Noen perspektiver bakover og fremover», *LOR* 1999, s. 170-188, med videre henvisninger.

28 Se f.eks. Lorents Rynning, *Allemandsret og særret*, Oslo 1928, s. 84: «Vor rettsorden hjemler ikke allemandsrettigheter som saadanne nogen klagerett eller 'actio'.»

29 Jf. bl.a. Rt. 1998 s. 1164 (Furumoa) s. 1170:»I allemannsrettene ligger … en viss begrensning av en eiers frie rådighet ….Han kan ikke egenrådig avskjære disse rettighetene, og enhver kan håndheve allemannsrettene.» (Min uth.)

30 Falkanger, op.cit., s. 174.

gjelder konkret allemannsretten i og rundt strandsonen, og det dynamiske elementet viser seg først og fremst gjennom måten Høyesterett i denne relasjon håndterer friluftslovens skille mellom innmark og utmark. Jeg skal gi to eksempler på dette:

> *Rt. 1998 s. 1164 (Furumoa): Spørsmål om strandsonen på privat eiendom var «innmark» eller «utmark» i friluftslovens forstand. Strandlinjen var 60 m lang, og avstanden mellom strandsonen og bolighuset var 65 m. Strandsonen var til sammen 11 m bred bestående av selve stranden (6 m) og et sivbelte (5 m). Det var bygget to moloer og en slipp på stranden opp i sivbeltet. Den ene moloen fungerte også som feste for en hengebro ut til et skjær med et bade-/gjestehus. I sivbeltet var det dessuten etablert noen mindre innretninger (utespiseplass, flaggstang mv.). Arealet mellom huset og strandsonen var opparbeidet med gressplen og busker. Strandsonen utgjorde et viktig oppholdssted for eierne og var mye benyttet av dem. Strandsonen ble av Høyesterett likevel anset som «utmark».*
>
> *Rt. 2005 s. 805 (Hvaler): En sti som ble benyttet av allmennheten gikk over privat eiendom og passerte 20 m fra eiendommens hovedhus og 7,5 m fra husets anneks. På fine sommerdager kunne det til dels være nokså stor trafikk på stien. Stien ble i sin helhet ansett å gå gjennom «utmark».*

Høyesterett tolker her utmarksbegrepet nokså liberalt. Det som er interessant i vår sammenheng er hvordan Høyesterett *begrunner* tolkningen. En grunnleggende uttalelse om dette finnes i Hvalerdommen der Høyesterett blant annet tolker begrepet «hustomt», som er et av kriteriene som gir et område status som innmark.[31] Førstvoterende uttaler her med tilslutning fra de øvrige dommerne at:

> *«Ved fastleggelsen av tomtebegrepet må det … blant annet tas hensyn til tomtens plassering. For allmennhetens behov for rekreasjon og friluftsliv står strandområder i en særstilling. Som følge av den store betydning slike områder har for allmennhetens friluftsliv må grunneiere som bygger i strandsonen, etter min oppfatning finne seg i å få allmennheten tettere inn på seg enn det som gjelder i områder hvor allmennhetens behov for ferdsel er mindre.»*[32] *(Min uth.)*

31 Se friluftsloven § 1a første ledd.

32 Rt. 2005 s. 805 (Hvaler), avsn. 62.

Når Høyesterett her trekker så snevre grenser for innmarksbegrepet, så er det altså ut fra den betraktning at eiendommen ligger i et område der friluftsinteressen står særlig sterkt. At Høyesterett på denne måten tøyer ordlyden ut fra reelle hensyn, er i og for seg ikke noe nytt. Det er imidlertid interessant å observere hvilken betydning friluftslovens *formålsbestemmelse* tillegges i Høyesteretts argumentasjon. Dette sies det noe om i den etterfølgende Ullrichsendommen, som konkret gjelder retten til *fortøyning, soling, bading* samt visse andre aktiviteter etter friluftsloven §§ 7, 9 og 11 – det vil si andre bestemmelser enn i Hvalerdommen. Ullrichsendommen gjentar imidlertid, sammen med Collettdommen, uttalelsen om at den som bygger i strandsonen må finne seg i å få allmennheten tettere innpå seg. Denne betraktningen synes derfor å ha *generell* relevans ved tolkning av friluftslovens bestemmelser. I Ullrichsendommen sies det dessuten følgende om betydningen av lovens formålsmestemmelse:

> *«Vedtakelsen av formålsbestemmelsen og den begrunnelse som ble gitt i den forbindelse, er en viktig bekreftelse på at det er rom for en dynamisk rettsutvikling på dette området også uten ytterligere medvirkning fra lovgivers side. … Samlet sett kan det neppe være tvilsomt at avveiningen av de motstående interesser i dag vil falle ut til fordel for allemannsrettene i større utstrekning enn ved vedtakelsen av friluftsloven»*[33]

Disse uttalelsene bekrefter etter mitt skjønn at formålsbestemmelsen har hatt en klar *egenverdi* for ivaretakelsen av allmennhetens interesser.

b Lånereglene

Spørsmålet er så hvordan *lånereglene* blitt forstått og anvendt i teori og praksis. For de fleste av lånereglene kan en slå fast følgende: De er *ikke unntaksregler* som skal tolkes innskrenkende. På den annen side er de *ikke rettigheter* i den forstand at de kan håndheves overfor opphavsrettshaveren. Man kan for eksempel ikke kreve fjernet en digital kopisperre alene på grunnlag av privatkopieringsregelen i åndsverkloven § 12. Reglene er heller *ikke preseptoriske*. De fleste lånereglene kan med andre ord fravikes i avtale mellom rettighetshaver og bruker.

33 Rt. 2007 s. 102 (Ullrichsen), avsnitt 79 og 85.

3 Drøftelse

3.1 Generelt

Gjennomgangen så langt har avdekket flere forskjeller mellom allemannsretten og lånereglene, men det er ikke derved gitt at opphavsretten har noe å lære. *Det* må som nevnt bero på om reglene om allemannsrett har løsninger som, anvendt på lånereglene, ville gi et alt i alt bedre opphavsrettslig regelverk. Jeg skal under dette punkt drøfte enkelte lærdommer som ut fra ovennevnte *kan* være aktuelle.

3.2 Mulig lærdom – Etablere et administrativt system for håndtering av konflikter mellom eier- og brukerinteresser

Én løsning, som det i prinsippet kunne være aktuelt å overføre til opphavsretten, er det administrative systemet for konflikthåndtering i friluftsloven kap. 2. Som vi har sett fins det der en rekke mekanismer for å avverge og avdempe konflikter mellom allemannsretten og eiendomsretten. Her kan det imidlertid innvendes at opphavsretten allerede *har* et konflikthåndteringssystem i åndsverkloven § 53b. I tillegg har åndsverkloven regler som pålegger brukere å opptre respektfullt og regler om erstatnings- og straffansvar ved rettighetsbrudd. Disse reglene gjenspeiler *noen av* virkemidlene i friluftsloven kap. 2.

Som nevnt kan mekanismen i § 53b hevdes å være utilstrekkelig. Det er imidlertid min vurdering at eventuelle forbedringer av denne mekanismen ikke bør bygges på allemannsrettens eksempel. Friluftslovens regler er her så spesifikt innrettet mot fast eiendom, at de etter mitt skjønn ikke passer i opphavsrettslig sammenheng. På denne bakgrunn kan jeg ikke se at opphavsretten her har noe å lære.

3.3 Mulig lærdom – Etablere en grunnleggende materiell distinksjon tilsvarende friluftslovens skille mellom inn- og utmark

En annen mulig lærdom er at den opphavsrettslige reguleringen kanskje kunne baseres på en tilsvarende grunnleggende distinksjon, som friluftslovens skille mellom inn- og utmark. Her kan det innvendes at dagens opphavsrett allerede bygger på en slik grunnleggende sondring – nemlig mellom *privat* og *ikke-privat* bruk. Både privat kopiering og privat tilgjengeliggjøring er som utgangspunkt unntatt fra opphavsrettshaverens kontroll.[34]

34 Jf. hhv. åndsverkloven §§ 2 og 12.

Riktignok *er det* blitt foreslått i opphavsrettsteorien at man i tillegg – eller i stedet – burde innføre et grunnleggende skille mellom *kommersiell* og *ikke-kommersiell* bruk.[35] Grunntanken bak en slik modell skulle være at ikke-kommersiell bruk skal være relativt fri for enhver, mens den kommersielle skal være forbeholdt opphavsrettshaveren. Etter mitt skjønn kan det imidlertid anføres tungtveiende innvendinger mot en slik løsning. For det første kan det være behov for å unnta *også visse former for kommersiell bruk* fra opphavsrettshaverens rådighet. Dette gjenspeiles i dagens låneregler, som også i noen utstrekning åpner for kommersiell bruk. For det annet er det vanskelig å se hvordan en skal kunne håndheve et slikt skille. Et DRM-system vil for eksempel vanskelig kunne bedømme om en forespurt kopieringshandling er kommersiell eller ikke. For det tredje kan det reises spørsmål *om det i det hele tatt finnes* ikke-kommersiell bruk i digital sammenheng. Digital teknologi setter rettighetshaveren i stand til å lisensiere nær sagt enhver bruk, og enhver bruk kan derfor sies å ha en potensiell kommersiell verdi *for rettighetshaveren*. Det lar seg derfor hevde at en for sterk vektlegging av skillet mellom kommersielt og ikke-kommersielt reelt sett vil *innsnevre* allmennhetens rettigheter i digital sammenheng.

Jeg vil på denne bakgrunn ikke anbefale et slikt tiltak.

3.4 Mulig lærdom – Anerkjenne lånereglene som rettigheter

En tredje mulig lærdom er å anerkjenne lånereglene som rettigheter. *Allemannsretten* kan sies å ha rettighetsstatus i den forstand at enhver kan håndheve den, for eksempel gjennom søksmål for domstolene. Å gi lånereglene en tilsvarende rettighetsstatus er generelt et mulig virkemiddel for å sikre dem gjennomslag i digital sammenheng. Jeg finner imidlertid ikke grunn til å gå nærmere inn på denne løsningsmodellen her, fordi jeg uansett finner at opphavsretten ikke kan lære noe *av allemannsretten* på dette punkt. Begrunnelsen er som følger: Når vi påpeker at allemannsretten kan håndheves, sikter vi til at enhver kan gå til sak for å få stadfestet f.eks. sin ferdselsrett over en bestemt grunneiendom. Som vi har sett, gir imidlertid ikke rettighetsstatusen noe vern mot at eieren endrer sin bruk av eiendommen, slik at allemannsretten *ikke lenger kan utøves der*. Rettighetsstatusen gir med andre ord ikke vern mot det vi kan kalle *faktiske* eiertiltak – og det er nettopp et *slikt* vern lånereglene trenger

35 Slik f.eks. Viveca Still, *DRM och upphovsrättens obalans*, Helsinki 2007; Jens Schovsbo og Thomas Riis, «Users' Rights: Reconstructing Copyright Policy on Utilitarian Grounds», *European Intellectual Property Review* 2007, s. 1-5.

i digital sammenheng. Det brukersiden der har behov for, er et vern mot at rettighetshaveren *faktisk* benytter DRM-teknologi til fortrengsel for låneregelene.

Etter min vurdering kan allemannsretten derfor ikke lære opphavsretten noe på dette punkt.

3.5 Mulig lærdom – Etablere offentligrettslige restriksjoner for faktiske eiertiltak som hindrer utøvelse av allmennhetens rett

I forlengelsen av dette kan man spørre om opphavsretten kan lære noe av tingsrettens mer generelle system med at endringer i bruken av fast eiendom er underlagt krav om samtykke eller andre offentligrettslige restriksjoner. Spørsmålet er om man kunne innføre tilsvarende restriksjoner for bruk av DRM-teknologi.

Planlovgivningens *samtykkekrav* er etter min oppfatning så spesialtilpasset fast eiendom, at *det* ikke lar seg overføre til opphavsretten. Derimot kunne en tenke seg et system med offentligrettslig *regulering* av bruken av DRM. Lovgiver kunne styre bruken av DRM gjennom konkrete forbud eller påbud knyttet til bestemte teknologier. En tungtveiende innvending mot en slik løsningsmodell er imidlertid at den fort ville bli *for statisk*: Man risikerer at teknologien allerede er utdatert før reguleringen trer i kraft. Reguleringsformen er dessuten blitt utprøvd i praksis uten at det har gitt særlig gode resultater, blant annet gjennom den amerikanske Audio Home Recording Act av 1992.[36]

Jeg finner derfor at opphavsretten heller ikke her har noe å lære.

3.6 Mulig lærdom – Innføre en formålsbestemmelse som understreker viktigheten av låneregelene og de hensynene de ivaretar

En siste mulig lærdom er å innføre en formålsbestemmelse, etter mønster av friluftsloven § 1, der lovgiver fremhever, og understreker viktigheten av, de hensyn låneregelene skal ivareta. Friluftslovens eksempel viser at en slik formålsbestemmelse vil kunne få stor betydning – både praktisk og prinsipielt – ved at den kan danne grunnlag for en befesting og utvikling av brukersidens rettigheter gjennom det praktriske rettsliv. En slik konkretisering og stadfesting av låneregelenes formål, og viktigheten av dem, ville også kunne gjøres på internasjonalt nivå. Man ville da blant annet få en *motvekt* mot den såkalte

36 Loven var ment å skulle regulere digital privatkopiering av musikk, men har gjennom rettspraksis fått innsnevret sitt virkefelt til kun å gjelde DAT-spillere – en teknologi som i de aller fleste situasjoner må anses som utdatert.

«tretrinnstesten», som er nokså dominerende i dagens internasjonale opphavsrett, og som nokså ensidig fremhever rettighetshaverens interesser. Å beskytte lånereglene gjennom en formålsbestemmelse – til forskjell fra mer direkte og pliktbasert regulering – ville dessuten gi et *fleksibelt* og *dynamisk* verktøy, som blant annet ville gi rom for å ivareta opphavsrettens mer overordnede funksjoner og målsetninger, ved avveiningen i den enkelte sak.

Min konklusjon er at opphavsretten, kanskje på dette *ene* punkt, kan ha noe å lære av allemannsretten. Det ville iallfall være verdt et forsøk.

4 Konklusjon

Gjennomgangen har avdekket en rekke forskjeller mellom allemannsretten og lånereglene. Flere av allemannsrettens løsninger vil etter mitt skjønn enten ikke passe for opphavsretten eller ikke tilføre den noe. På *étt* punkt kan imidlertid opphavsretten kanskje lære noe, og det er i friluftslovens formålsbestemmelse. Å innføre en tilsvarende formålsbestemmelse for lånereglene *kan* etter min vurdering gi et alt i alt bedre opphavsrettslig regelverk.

LEGAL ISSUES REGARDING WHOIS DATABASES[1]

Dana Irina Cojocarasu

Introduction

The domain name system (DNS) assists users of the Internet in navigating the network by translating Internet Protocol (IP) addresses, which are numeric, into conventional denominations more easily recognised and remembered by the users. A prerequisite for such a translation, however, is that the alphabetical identifiers are unique. In response to the need for maintaining the integrity of names already registered (thus ensuring that every name in the DNS is unique), the «WHOIS» service was created. In broad terms, WHOIS is a service which allows interested parties to address queries to databases (WHOIS databases) containing information about registered domain names, their registrants and the servers they use. Originally, the provision of the service was voluntary for both the registries responsible for managing and allocating domain names and the domain name registrants. The latter had the option of making their contact information available to their peers by registering themselves in a WHOIS database. Subsequently, the functionality of the service was expanded by enabling inquiries about the status and availability of a domain name. Nowadays, in response to a query to a WHOIS database, one is given access to information about one or more registered domain names, the identity of the registrants and the associated servers. The purpose of storing and displaying this information is to enable communication with a party responsible for the domain name in question or with a party that can reliably hand on data to a party that is able to resolve issues concerning the configuration of the records linked to the domain name.[2]

Taking as a point of departure the purpose of the WHOIS service, the goal of this report and the research behind it is to examine the roles and responsibilities of the actors involved in the creation and management of the WHOIS databases and to investigate the policies involved in the collection, processing

---

1 Originally published in the report *Legal issues regarding WHOIS databases* / Dana Irina Cojocarasu. - Oslo :Norwegian Research Centre for Computers and Law : Unipub, [2009]. - (Complex ; nr. 2/2009).

2 See generally GNSO Whois Task Force, *Final task force report on the purpose of WHOIS and of WHOIS contacts* (15.03.2006), <http://gnso.icann.org/issues/whois-privacy/tf-report-15mar06.htm#0.1>.

and transfer of the information contained in WHOIS databases in selected top-level domains (TLDs).[3]

This report builds on a basic distinction between the policy model applicable to generic TLDs (gTLDs) and that of country-code TLDs (ccTLDs). This distinction has implications, in the given context, for which of the (public) authorities have the competence to decide upon and to implement the policies for the provision of WHOIS service and for the functioning of WHOIS databases. The distinction also has an impact on the enforcement mechanisms that can be implemented in the event that agreed rules are infringed.

In very general terms, the Internet Corporation for Assigned Names and Numbers (ICANN) is a non-profit corporation with functions relating to, among other areas, Internet Protocol (IP) space allocation, and gTLD name system management. ICANN has a de facto monopoly on establishing the policies that regulate the gTLDs. These policies are created subsequent to a decision-making process resulting in a consensus between the views of the supporting organisations and constituencies and those of the international Internet community (as expressed during the public review of the policy documents). In addition, ICANN has entered into direct agreements with the registries designated to operate each gTLD and has set up an accreditation procedure for registrars (i.e., those who carry out the actual registration of domain names) wishing to provide registration services to interested parties.

On the other hand, the management of country-code top-level domains is now assigned by ICANN to countries or regions and is primarily governed by rules established at national level.[4] According to the principles and guidelines for the delegation and administration of ccTLDs suggested in 2005 by the Governmental Advisory Committee for ICANN, «ccTLD policy should be set locally, unless it can be shown that the issue has global impact and needs to be resolved in an international framework».[5]

A registry for a ccTLD is typically appointed by its national government and the local Internet community to operate the namespace concerned. The registry and ICANN usually exchange formal letters of collaboration (or enter into a separate agreement), expressing a mutual commitment to cooperate in order to ensure the stable and secure operation of the Internet's unique identifier systems for the benefit of the Internet users. Subsequently, the national registry will set up

3 The concept of «top-level domain» and related concepts in the DNS are explained in Chapter 1.

4 See further, e.g., Lee A. Bygrave & Jon Bing (eds.), *Internet Governance: Infrastructure and Institutions* (Oxford: Oxford University Press, 2009), chapter 5 (sections 5.1.4, 5.4, 5.5).

5 Governmental Advisory Committee, «Principles and guidelines for the delegation and administration of country code top level domains» (Mar del Plata, 05.04.2005), <http://gac.icann.org/web/home/ccTLD_Principles.rtf>.

policies for the accreditation of registrars and will stipulate conditions regulating how registrars may provide registration services under the national domain.

The normative framework for the provision of WHOIS service at the gTLD level is currently under review. Significant changes in the rules for the collection, use and transfer of the information stored in the WHOIS databases have been proposed in order to better meet the requirements of privacy and data protection legislation, to improve the accuracy of the information stored in the WHOIS databases and, at the same time, to cater for the legitimate interests of various stakeholders. This process has come to a temporary halt at gTLD level due to the difficulties encountered in reaching a broad international consensus.[6] While not directly affected by the gTLD policy process, the managers of European ccTLDs, like all ccTLD managers, continually face the challenge of implementing a WHOIS service that duly takes into account the needs of all the stakeholders legitimately interested in access to the WHOIS databases, while also complying with the obligations assumed through bilateral agreements in accordance with the law.

It is in this international climate that the analysis in this report takes place. In order to convey a multi-faceted image of WHOIS service, research was focused primarily on three business models: one applicable to domains registered at a gTLD level (.com) and the other two applicable to selected domains registered at ccTLD level (.no and .eu). The latter two models, however, differ from one another (although the domains are situated at the same hierarchical level in the DNS). Registration under the .eu domain is open for all citizens and organisations in the European Union and, by contrast to .no (or any other national domain), .eu functions according to rules set up at a supranational (as opposed to national) level.

In addition to its academic significance – as one of the few extensive legal analyses of a key service in the Domain Name System – the present report may serve as a practical contribution to management of the .no domain by identifying the benefits and shortcomings of the current policy model for that domain (as compared to the policies for .com and .eu) and by suggesting an improved framework with additional legal safeguards for the stakeholders involved.

The WHOIS service cannot be regarded as a stand-alone service, since it is meant to function as a support for the current DNS. Thus, in order to put provision of the service in its proper legal context, relevant elements of domain name management are explored in Chapter 1. Special focus is devoted to the decision-making processes and actors in the DNS, including the relevant agreements reached and their enforcement mechanisms.

6 *Whois Study Group Report to the GNSO Council* (22.05.2008), <http://gnso.icann.org/issues/whois/gnso-whois-study-group-report-to-council-22may08.pdf>.

Following a presentation of some key stages in the evolution of the WHOIS service, Chapter 2 examines the features and functions of WHOIS databases. The discussion in Chapter 2 sets the premises for evaluating the effectiveness of the WHOIS regime in safeguarding the privacy interests of the domain name registrants. It is argued that by clearly defining the purpose(s) of the WHOIS databases, the registries and registrars would be able to ensure that legitimate goals are pursued through collecting only the minimum necessary amount of personal data from registrants. Chapter 2 focuses, therefore, on the possible legitimisation – de jure or de facto – of publication on the Internet of the registered information about the domain name and its registrant. If WHOIS databases are to function effectively, the input data must be accurate throughout the period during which the domain is active. Analysis of the agreements entered into by the registries, registrars and the domain name registrants discloses several challenges in terms of ensuring a high level of accuracy of the data fed into WHOIS databases.

Under the compulsory agreements entered into by the registries and registrars at the gTLD level, the provision of WHOIS service is obligatory. Registries and registrars are required to set up and to provide access to WHOIS databases, free of charge via the web and port 43, and with remuneration via bulk-access agreements with third parties. In the case of national (.no) and regional (.eu) TLDs, the decision regarding the content of, and access to, WHOIS data is made at the local level and published through the relevant domain name policies. Taking into account that the WHOIS service involves access to WHOIS databases created and managed by the registry (in the ccTLDs) or the registrars (in the gTLDs), Chapter 3 identifies the scope of the registries'/registrars' respective intellectual property rights in WHOIS databases as well as the consequences this has on the functioning of WHOIS service.

Subsequently, Chapter 4, the most extensive part of the study, addresses the «Gordian knot» of the policy reform process at gTLD level – that is, the content of the WHOIS databases. More precisely, it investigates the rights and obligations of the registries and registrars in lawfully processing the personal data submitted upon registration of the domain name. The chapter identifies the main requirements of the European data protection laws and illustrates how they can be understood as guarantees that should remain paramount during the provision of WHOIS service. Best practice examples are extracted from the existing regimes at ccTLD level, as well as from the proposals that were submitted during the consensus-building process at gTLD level. In the light of the legal requirements and of the existing practice, an argument is made out for the implementation of a layered access to WHOIS databases responding to the legitimate needs of potentially interested parties (as identified in Chapter 2) by providing only such information as is necessary and sufficient

for the attainment of the specific purpose of the query. This argument is based on a reconciliation between the privacy interests of the registrant and the informational needs of the requestor.

However, when the query is made in conjunction with law enforcement, societal interests may outweigh the personal interests of the registrant. As detailed in Chapter 5, access to information for legitimate law enforcement purposes should be facilitated, and well-defined routines should be in place to enable access and exchange of information between international law enforcement agencies. In this manner, the apparent dichotomy between privacy and disclosure could be replaced by the acknowledgement of the idea that a privacy-friendly WHOIS policy may lead to increased accuracy in the database and facilitate, in turn, the legal pursuit of those who abuse the domain name system and misuse WHOIS data.

1 The Domain Name System: Normative Framework

The domain name system (DNS) was conceived as a distributed mechanism to transpose domain names – that is, user-friendly, alphabetic names for Internet sites (e.g., www.uio.no) – into numeric Internet Protocol (IP) addresses (e.g., 203.160.185.48). Domain names are divided by «dots» and hierarchically structured from right to left. At the top of the hierarchy lie the top-level domains (TLDs). These are the last label on the right-hand side of the dot furthest to the right in the domain name. Next in the hierarchy is the second-level domain (SLD) which is represented by the label situated immediately to the left of the «dot» before the TLD. For example, in the designation «uio.no», the «uio» element represents the second level while «.no» denotes the TLD reserved for Norway.

The TLDs are divided into two classes: generic top-level domains (gTLDs) (e.g., .com, .org, .net, .biz, .info, .name) and country-code top-level domains (ccTLDs). While an exhaustive description of the domain name system exceeds the scope of this research project and report, the distinction between gTLDs and ccTLDs is essential because it entails differences in both the applicable policies and the decision-making procedures for domain name registration and management of registrant data. As a consequence, the policies for WHOIS databases differ for ccTLDs and gTLDs respectively. Moreover, as explained in the following sections, the competence of the rule makers for gTLDs differs from that of ccTLD managers.

This chapter provides insight into the policy framework for the Internet domains situated at the highest level of the DNS hierarchy. Understanding this framework is crucial. The starting point of any regulatory intervention, whether it is shaped as a self-regulatory process or as a legal statute, is the fulfilment of a

policy objective. The policy objective is usually expressed in the form of guiding principles for the activity to be regulated. Once agreed upon, these principles serve as a basis for setting up rules and standards and, indirectly, for defining activities and circumstances under which a violation of the rules/standards can be deemed to have occurred. The final component of a standard regulatory process entails the integration of the regulatory act in an enforcement context (for example, by determining the bodies competent to decide whether a violation has taken place and which are authorised to impose appropriate sanctions).

In analysing the scope of the substantive rights and obligations pertaining to WHOIS databases and the information contained therein, extensive reference is made in the following to the provisions of several national and international policy documents representing the legal basis of such rights and obligations. Most often these policy instruments are the result of a self-regulatory intervention of the stakeholders themselves, rather than a governmental intervention. Examining their legitimacy, the scope of their applicability as well as possible conflicts among them is a major task of the research. Moreover, where statutory regulation applies, it is vital to identify the applicable law for a given domain.

1.1 gTLD policy development process

Responsibility for managing the DNS inheres primarily in the Internet Corporation for Assigned Names and Numbers (ICANN). This is a non-profit organisation headquartered in California but with an international membership. Under ICANN's aegis, the multitude of various stakeholders in the DNS can have a say in the administration of that system and other aspects of the Internet.

According to Article I section 1 of its Bylaws,[7] ICANN's mission is «to coordinate, at the overall level, the global Internet systems of unique identifiers, and in particular to ensure the stable and secure operation of the Internet's unique identifier systems». In addition to performing technical functions, ICANN coordinates the development of policies inasmuch as they relate to these functions. The legitimacy of ICANN as a policy maker is said to derive from the direct involvement of different categories of stakeholders represented within the organisation through both elected bodies and nominated representatives, as well as committees, councils and supporting organisations.

Formally, ICANN's top policy decision body is the Board of Directors. The Board consists of fifteen voting members (Directors) and six non-voting

7 The ICANN Bylaws have been amended several times since 1998. The version used for this research project was effective as of 29.05.2008. It is available at: <http://www.icann.org/en/general/bylaws.htm>.

liaisons (Article VI section 1 of the Bylaws). The composition of the Board is intended to reflect cultural and geographic diversity as well as a solid understanding of the potential impact of ICANN decisions on the global Internet community (Article VI section 3).

The decisions of the Board are typically based on policy recommendations that are thrashed out and agreed upon by one or more of ICANN's Supporting Organisations and Advisory Committees (described immediately below), in accordance with their respective mandate.

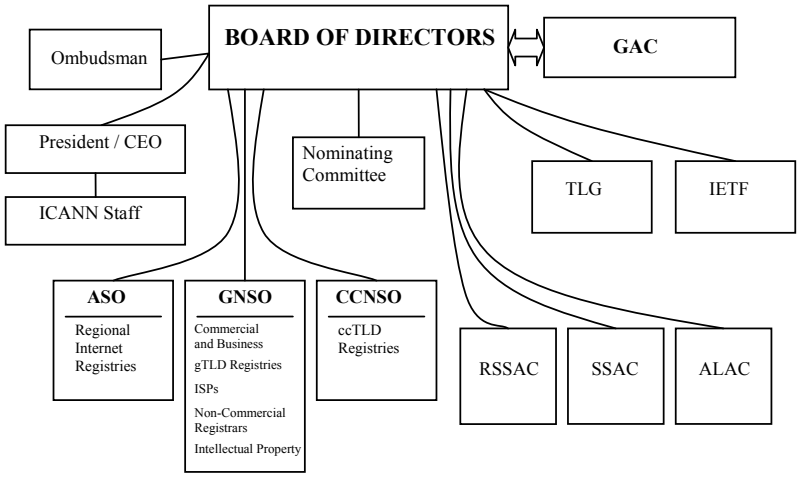


Figure 1. ICANN structure[8]

The Supporting Organisations are consultative and policy development bodies allowing multiple stakeholders in the global Internet community to contribute to policy making on matters that fall within ICANN's area of competence. The consensus reached on policy matters within one of the Supporting Organisations is duly considered in the final decision taken by the Board.

In the context of this study, the most important of the Supporting Organisations is the Generic Names Supporting Organisation (GNSO). This body is responsible for developing and recommending substantive policies applicable at gTLD level. Reference is made to the GNSO throughout this report since the organisation is leading the policy reform for the gTLD WHOIS databases. The GNSO has also been instrumental in the development of the

8 Taken from Bygrave & Bing (eds.), *Internet Governance*, *op. cit.*, p. 107. There one finds also an explanation of the various acronyms and the organisations they represent.

Uniform Domain Name Dispute Resolution Policy,[9] the addition of new gTLDs and the protection of trademarks in the new TLDs. The GNSO comprises seven constituencies, representing the gTLD registries, registrars, Internet Service and Connectivity Providers, commercial and business users, non-commercial users and the interests of intellectual property rights holders.

The Country Code Names Supporting Organisation (ccNSO) develops and recommends global policies regarding ccTLDs, nurturing consensus across the ccNSO community and coordinating with other ICANN-supporting organisations. The technical administration as well as the policy making at ccTLD level have been delegated by ICANN to the national ccTLD managers (national registries). As a consequence, the policy competence of ccNSO is restricted (in accordance with Annex C of the Bylaws) to:

- developing best practice for ccTLD managers in order to ensure interoperability at a ccTLD level; and
- initiating generic policies delineating the division of competence between ICANN and the national decision-making authorities (governments and national registries).

The ccNSO is made up of those ccTLD managers (registries) that have agreed in writing to become members of it.

The third Supporting Organisation is the Address Supporting Organisation (ASO). This advises the Board on policy issues relating to the operation, assignment and management of Internet addresses.

In addition to the Supporting Organisations, several Advisory Committees have been created under the aegis of ICANN. These are the Governmental Advisory Committee (GAC), Security and Stability Advisory Committee (SSAC), Root Server System Advisory Committee (RSSAC) and At-Large Advisory Committee (ALAC). Although these committees have no legal authority to act for ICANN (Article XI section 1 of the Bylaws), their findings and recommendations are reported to the Board. The most influential committee (with respect to the Board) is GAC, which is made up of representatives of national governments, intergovernmental organisations (the International Telecommunications Union (ITU) and World Intellectual Property Organisation (WIPO)), the European Commission and other regional bodies. GAC provides advice particularly whenever there might be interaction between ICANN policies and existing national laws and international agreements or whenever public policy issues could be raised. For example, GAC has drafted the «Principles

9 For a brief description of this policy, see Bygrave & Bing (eds.), *Internet Governance*, *op. cit.*, section 5.2.2.

and guidelines for the delegation and administration of the ccTLDs»,[10] broadly recognised as the framework for delineating the relative competence of ICANN from that of national governments and national registries. The Committee may propose issues for consideration to the ICANN Board either directly, by way of comment and prior advice, or indirectly, by recommending an action or a new policy development process, or by initiating the revision of existing policies. Although the views of GAC are not binding on the ICANN Board, the latter is obliged to find a mutually acceptable solution in the event that it wishes to act in a way that is inconsistent with GAC advice (Bylaws Article XI section 2(1)(j)).

Another significant committee (at least in respect of the issues taken up in this report) is the At-Large Advisory Committee (ALAC). This was founded to consider and provide advice on the activities of ICANN insofar as they relate to the interests of the individual Internet users. Obviously, ALAC may play a part in policy discourse on WHOIS issues, primarily as a voice for the concerns of individual Internet users in their capacity as WHOIS database registrants.

The substantive policies developed by ICANN for the gTLDs are the result of a self-regulatory process known as the GNSO's Policy Development Process (PDP). The process, described in Annex A of the Bylaws, aims at achieving legitimacy through ensuring that those entities most affected by it can assist in creating the rules they are supposed to apply.[11] A diagram of the GNSO's PDP is reproduced in Figure 2. Beyond the typical stages illustrated in the diagram, other intermediary procedures may be decided by the GNSO Council[12] when needed, such as, for example, the creation of a Working Group in order to improve and elaborate the recommendations in the Task Force Reports or additional public consultations.

The main features of the PDP are as follows:

1. It strives to ensure that the various stakeholders are represented in the decision-making process. The GNSO Constituencies, representing various groups of affected parties, have the opportunity to appoint representatives to both the GNSO Council and the GNSO Task Force. While the Council is competent to initiate the policy process, the Task Force gathers relevant information documenting the positions[13] of the Constituencies «as spe-

10 Referenced *supra* note 4.

11 See the core values of the ICANN decision-making process and actions as described in Article I section 2 of the Bylaws.

12 This is the case for the current discussions regarding the reform of WHOIS policies. See particularly «GNSO Consideration of Proposed Changes to WHOIS» (14.09.2007), <http://www.icann.org/en/announcements/announcement-2-14sep07.htm>.

13 See Bylaws Annex A paragraph 7(d)(1) for details regarding the compulsory contents of a Constituency Statement.

cifically and comprehensively as possible, thereby enabling the Council to have a meaningful and informed deliberation on the issue» (Bylaws Annex A paragraph 7(a)). In addition, the Task Force can solicit the input of external advisors, experts or members of the public.[14] Their views expressing assent or dissent will be included in the Task Force Reports. Moreover, two Public Comments sessions, each lasting 20 days, ensure that the relevant opinions of other interested parties not represented in ICANN are considered in the final decision of the ICANN Board.

2. It provides for well-informed rule making. First of all, reasoning must be given for all Constituency Statements (Bylaws Annex A paragraph 7(d)(1)). Moreover, again in accordance with the Bylaws, the level of consensus reached (supermajority vote, consensus, and dissenting opinions) must be documented; the same applies to the implementation issues identified. In addition, the outside experts or advisors involved must state in detail their qualifications and relevant experience as well as potential conflicts of interest that may influence their opinion. The Final Report of the GNSO Council (the «Board Report»), based on the conclusions of the Task Force report and the results of the Public Comments Sessions, informs the ICANN Board not only about the broad consensus reached but also, if applicable, all the dissenting opinions of the Council Members and their reasoning.
3. Being the result of mutual consultation and agreement, the policy transcends jurisdictional issues. The consensus policies resulting from the PDP apply to all the gTLDs, and are meant to be implemented by all ICANN-accredited registrars[15] (under the potential sanction of having their accreditation withdrawn) as well as the registries[16] designated by ICANN to manage gTLDs.
4. The PDP ensures flexibility in the adoption and modification procedures in the sense that the procedures for policy making may be amended or modified following a proposal from the GNSO Council, subject to the subsequent approval by the ICANN Board (Bylaws Article X section 3(4)). Moreover, as reflected by the PDP for WHOIS databases, if the GNSO

14 An independent report commissioned by ICANN to examine its accountability and transparency practices, has pointed out, however, that the corporation should make additional efforts to explain more clearly how input is used when making decisions, in order to ensure consistent engagement of the public. See One World Trust, *Independent Review of ICANN's Accountability and Transparency – Structures and Practices* (London, March 2007), <http://www.icann.org/en/transparency/owt-report-final-2007.pdf>.

15 See Section 4 of the Registrar Accreditation Agreement (17.05.2001), available at <http://www.icann.org/en/registrars/ra-agreement-17may01.htm>.

16 See Article III section 3(1)(b)(i) of the .com registry Agreement (01.03.2006) (available at <http://www.icann.org/en/tlds/agreements/com/>) and corresponding provisions in similar agreements for other gTLDs.

Council considers that the Final Task Force Report leaves certain conceptual or implementation issues unanswered, it can decide to convene another Working Group to further elaborate the conclusions reached by the Task Force, this prior to submitting a Final Proposal to the ICANN Board.

5. The Bylaws provide several guarantees for ensuring that the PDP is transparent from inception to implementation. Throughout the PDP, ICANN will maintain a status web page on its website, detailing the progress of each PDP issue and describing (see Bylaws Annex A paragraph 15):
   a. The initial suggestion for a policy;
   b. A list of all suggestions that do not result in the creation of an Issue Report;
   c. The timeline to be followed for each policy;
   d. All discussions among the Council members regarding the policy;
   e. All reports from task forces, the Staff Manager, the Council and the Board; and
   f. All public comments submitted.

The result of the PDP is a Consensus Policy, which is compulsory for both accredited registrars and gTLD registries, regardless of the national jurisdiction under which they otherwise function. ICANN remains thus the sole actor with policy-making competence in gTLDs whereas registries and registrars are only called upon to implement and comply with existing and future policies developed through a PDP, as well as with Temporary Specifications or Policies adopted by the ICANN Board.[17]

To date, two consensus policies have been adopted by the ICANN Board concerning WHOIS:

- The WHOIS data reminder policy (27.03.2003);
- The WHOIS marketing restriction policy (12.11.2004).

The Board has also adopted a policy for dealing with potential conflicts between WHOIS requirements and privacy laws (10.05.2006).[18] These policies are elaborated in Chapters 2 and 4.

17 Article III section 3(1)(a)(i) of the .com registry Agreement (01.03.2006).

18 As far as I understand, although the latter policy was endorsed by the ICANN Board through a formal procedure, this cannot be regarded as a fully-fledged Consensus Policy in the same way as the other two policies (marketing restriction and data reminder) because it does not impose any new obligations on any registries, registrars or third parties and it is intended only to guide ICANN's response to potential difficulties that its contracting parties could have in complying with ICANN contractual requirements.

As for the issues of collection, public display and transfer of WHOIS data, these have been the subjects of a consensus-building process for several years. However, a final decision on these issues has not yet been taken by the ICANN Board, so the rules in force for dealing with them still stem from ICANN's practice and its binding agreements with the accredited registrars and the gTLD registries rather than from a consensus process as the one described above.

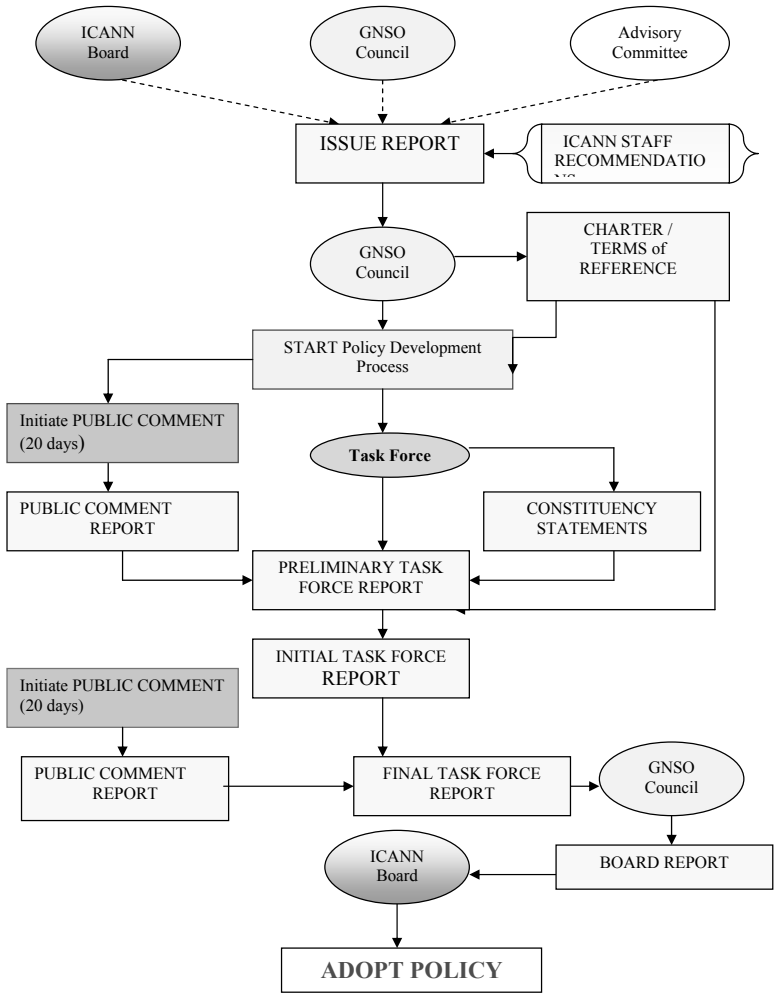


Figure 2. GNSO Policy Development Process

1.2 ccTLD policy development process

A country-code top level domain (ccTLD) is a domain used by and reserved for a country or a dependent territory. It is expressed in two-letter country codes mostly based on the ISO 3166-1 standard[19] (e.g., .no for Norway or.au for Australia). The country's top-level domain[20] is often viewed as the flagship of a country's Internet participation and as a strategic asset with symbolic, socio-economic and/or Internet stability and security implications.[21] Country-code TLDs were originally delegated in order to allow local Internet communities worldwide to develop their own locally responsive and accountable DNS services.[22]

1.2.1 ICANN's role in policy development at ccTLD level

As described in section 1.1.1 above, ICANN retains sole policy-making authority for the gTLDs. The question this section wishes to answer is to what extent policies developed by ICANN primarily for the gTLDs can be imposed upon the managers of the ccTLDs, in addition to or despite rules set up at a national level. This question becomes relevant especially given the current policy development process started by ICANN on the provision of WHOIS services and on the management of access to the personal data contained in WHOIS databases.

First and foremost, ccTLD issues are addressed under the aegis of ICANN within the ccNSO. This Supporting Organisation is opened to voluntary membership from ccTLD national managers.[23] In accordance with ICANN Bylaws

19 According to this definition, .eu is technically not a ccTLD.

20 Historically, most ccTLDs were operated by academic organisations. In most cases, governments retain direct control over, or have instituted a formalised relationship with their national ccTLD operators. Most have established a subsidiary company of a government ministry or have entered into operational contracts with their national ccTLD registry through which they assert their ultimate authority. Only in a few countries have the governments insisted upon total control over TLD management, enacting specific legislation granting themselves final authority over their ccTLDs and setting out registration requirements (the case in Spain, Finland and Greece). In a similarly small number of countries (Germany, UK), there is no formal governmental role in their respective ccTLD at all. Their registries, in other words, act without direct statutory basis and independently of direct state control.

21 See OECD Working Party on Telecommunication and Information Services Policies, *Evolution in the management of Country-Code Top-Level Domain Names (ccTLDs)* (DSTI/ICCP/TISP(2006)6/FINAL; 17.11.2006), available at: <http://www.oecd.org/dataoecd/8/18/37730629.pdf>.

22 See particularly RFC 1591: Domain Name System Structure and Delegation (March 1994), <http://www.ietf.org/rfc/rfc1591.txt>.

23 NORID became a member of ccNSO on 06.12.2006.

Article IX section 4(10), an ICANN policy shall apply to ccNSO members (by virtue of their membership) if certain cumulative conditions are met:

1. regarding the scope of the policy: it should address issues under the field of competence of ccNSO (a field which takes account of ccTLDs but which requires overall coordination from ICANN);[24]
2. regarding the adoption procedure:
   - the policy has been developed through a ccPolicy Development Process as described in Annex B of the Bylaws;
   - following the recommendation of the ccNSO, the policy has been adopted by the Board.

Over and above these conditions, ICANN polices shall not be imposed upon the ccNSO members when they conflict with the national law applicable to the ccTLD manager. The national law «shall, at all times, remain paramount» (Bylaws Article IX section 4(10)).

The above provisions in the Bylaws were introduced following a reform process initiated by the Governmental Advisory Committee (GAC). The process aimed at improving and better emphasising the division of responsibility between ICANN, national governments and the national registries regarding policy making for ccTLDs. The consensus reached within GAC on this point is expressed in its document «Principles and guidelines for the delegation and administration of country code top level domains».[25] The document represents the views of the national governments, distinct economies, multinational governmental and treaty organisations that are members of the GAC. The Principles are intended as a guide to the relationships between governments, their ccTLDs and ICANN; as such they are not meant to be binding.

The guiding principle in policy making at ccTLD level is that of subsidiarity – ccTLD policy should be set locally, by the local Internet Community, according to national law. Only exceptionally can a global approach be encouraged by ICANN, provided it can be shown that the issue has global impact and needs to be resolved in an international framework. This global approach is now pursued within the scope of ccNSO's activity.

The following figure depicts the relative division of policy-making authority among national governments, national registries and ICANN, as recommended by the 2005 GAC principles.

24 According to Bylaws Article IX section 6 and Annex C.
25 Referenced *supra* note 4.

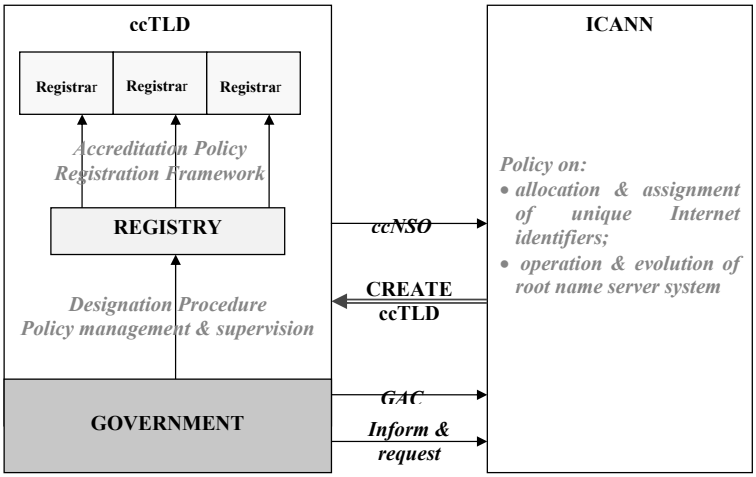


Figure 3. The division of policy-making competence at ccTLD level

1.2.2 Policy-making role of national authorities

In contrast to the situation for gTLDs, the policy-making competence regarding ccTLDs is shared between the relevant government or public authority and the registries. The national rule-making authority has the competence to set up the general policy rules applicable to the national domain in question. This high-level framework shall set up requirements for the domain name policy development process for each top-level domain, the minimum requirements that need to be met by a registry administering a top-level domain, and the consequences if those requirements are not met. In Norway this function is primarily performed by the Norwegian Ministry of Transport and Communications which sets the framework in a Regulation on domain names.[26] In the case of the .eu registry, the highest policy-making competence for defining the framework for domain name administration and the rules for the registration of domain names is assigned to the European Commission. In

26 Regulation No. 990 of 01.08.2003 on domain names under Norwegian country code top-level domains (Forskrift om domenenavn under norske landkodetoppdomener). The statutory basis for the Regulation is the Electronic Communications Act (Act No. 83 of 04.07.2003) sections 7-1 and 10-1.

Commission Regulation (EC) No. 874/2004 of 28.04.2004,[27] the Commission lays down public-policy rules concerning the implementation and functions of the .eu TLD and the principles governing registration under that domain.

As stated in the World Summit on Information Society (WSIS) Declaration of Principles of December 2003, the «policy authority for Internet-related public policy issues is the sovereign right of States. They have rights and responsibilities for international Internet-related public policy issues» (paragraph 49(a)). This statement is repeated in the WSIS Tunis Agenda for the Information Society of November 2005 paragraph 35.[28] Further, the WSIS Plan of Action of December 2003 invites Governments «to manage or supervise, as appropriate, their respective country code top-level domain name» (paragraph 13(c)(ii)). Working in collaboration with their local Internet community and considering the appropriate national laws and policies, governments are given a clear to mandate to decide on the rules for the designation of an appropriate manager for the national ccTLD.

The policy-making competence of the national government, absolute within the boundaries of its jurisdiction, is exercised in this field through the recognition of its right to make decisions concerning:

- requests to ICANN that its appropriate country code be represented as a ccTLD in the DNS;
- designation of the registry for the ccTLD concerned;
- the manner in which the core values of the domain name management should be transposed into policy principles to be followed in the accreditation of registrars and in the allocation of domain names.

1.2.2.1 Policy-making role of registries

Within the national framework thus set, the designated national registry will draw up the detailed policies concerning the accreditation of registrars as well as the registration of domains under the national domain name. Further, the ccTLD registry will provide a name service to the local Internet community in its jurisdiction, and according to a name policy as decided by the local community (including the government).

27 Set out in Official Journal of the European Communities (hereinafter «O.J.») L 162, 30.04.2004, pp. 40–50.

28 Cf. paragraph 63 of the Tunis Agenda: «Countries should not be involved in decisions regarding another country's country-code Top-Level Domain (ccTLD). Their legitimate interests, as expressed and defined by each country, in diverse ways, regarding decisions affecting their ccTLDs, need to be respected, upheld and addressed via a flexible and improved framework and mechanisms».

Take, for example, the role of EURid, which is the registry for the .eu domain. Under Article 4 of Regulation No. 733/2002 of 22.04.2002 on implementation of the .eu Top-Level Domain,[29] EURid is charged with the organisation, administration and management of the .eu TLD, including maintenance of the corresponding databases and the associated public query services, the accreditation of registrars, the registration of domain names applied for by accredited registrars, the operation of the TLD name servers and the dissemination of TLD zone files. In addition to this operative role, the registry shall organise, administer and manage the .eu TLD in the general interest and on the basis of principles of quality, efficiency, reliability and accessibility and it shall define and implement an extra-judicial settlement of conflicts policy. The registry shall also enter into accreditation agreements with registrars, defining the terms under which they have the right to register domain names under the ccTLD.

1.2.2.2 Scope of registrar's decision-making competence

A registry has a responsibility for shaping the registration regime so that the service it offers (registration of domains) abides by the domain name policy set by the regulatory authorities. This function includes defining the border between the tasks that should be centralised at registry level, and the tasks that should be handed over to registrars.

In the .no domain name policy, for instance, a registrar submits on behalf of an applicant an application to register a domain name under the domains that Norid manages in its role as registry. The registrar is obliged to comply with the regulations in effect at any time, as well as the guidelines and routines that Norid has provided on its Web pages. The registrar's decision- making competence is restricted to designing its own internal routines to best ensure compliance with the framework set by Norid while at the same time being economically efficient.

Similarly, each registrar accredited under the .eu domain shall be bound by contract with the registry to observe the terms of accreditation and in particular to comply with the public policy principles set out in the domain name policy. Registrars may also develop label, authentication and trustmark schemes. These schemes are regarded as a useful instrument for promoting consumer confidence in the reliability of information that is available under a domain name they registered, as well as a guarantee for compliance with applicable national and Community law.[30]

29 O.J. L 113, 30.04.2002, pp. 1–5.
30 Commission Regulation (EC) No. 874/2004, Article 5.

KRAV TIL FELLESKOMPONENTER SOM INFORMASJONSINFRASTRUKTUR[1]

Erik Hornnes, Arild Jansen og Øivind Langeland

Abstrakt

Med utgangspunkt i Regjeringens beslutning om å legge en felles IKT-arkitektur til grunn for forvaltningens IKT-løsninger, drøfter artikkelen noen sentrale utfordringer i dette arbeidet. Den teoretiske basisen for diskusjonene er vår forståelse av informasjonsinfrastrukturer, med vekt på begreper som installert base, kultivering og bootstrapping. Samtidig ser vi at en mulig felles informasjonsinfrastruktur for forvaltningen også må baseres på andre prinsipper og oppfylle flere behov enn tradisjonelle typer infrastrukturer, og være tilpasset den enkelte nasjons spesifikke forvaltningspolitikk og styringspraksis. Vi introduserer en ny kategori: forvaltningsinfrastruktur og skisserer noen krav til en framtidig norsk forvaltningsinfrastruktur, som vi mener også vil ha en relevans for tilsvarende arbeid i offentlig forvaltning i andre land.

Keywords: IKT-arkitektur, informasjonsinfrastruktur, forvaltningspolitikk, kultivering

1 Innledning

Regjeringen har høye ambisjoner knyttet til det offentliges bruk av IKT. Et sentralt virkemiddel er å legge en felles IKT-arkitektur til grunn for utvikling av nye eForvaltningsløsninger. Dette skal blant annet bidra til at borgere og næringsliv møter en mer samordnet og brukervennlig offentlig sektor (Difi 2009)[2]. Å etablere et slikt helhetlig rammeverk som det den felles IKT-arkitekturen representerer, er i tråd med hva en rekke andre land gjør, både i og utenfor Europa (Janssen og Hjort-Madsen 2007; Liimatainen 2008). Ut fra et teknologisk perspektiv synes tiden å være moden for dette. Men samtidig innebærer innføring av en felles IKT-arkitektur en rekke utfordringer, både

1 Paper til konferansen Nokobit 2009, 23.-25.november i Trondheim. Under publisering.

2 Se også St.meld. nr. 17 (2006-2007) Eit informasjonssamfunn for alle og St.meld. nr. 19 (2008-2009) Ei forvaltning for demokrati og fellesskap.

knyttet til tekniske, organisatoriske og ikke minst rettslige forhold. Det norske forslaget til en slik felles IKT-arkitektur omfatter også tiltak som i noen grad har vært foreslått og til dels forsøkt gjennomført tidligere, men som man av mange årsaker ikke har lykkes med (se f eks. Haraldsen 2003, Jansen 2008)[3]. Det synes derfor nødvendig å klarlegge hvilke spesifikke forutsetninger som må ligge til grunn for å lykkes i dette arbeidet, og hvordan det kan realiseres i praksis. Her kan både tidligere erfaringer være nyttige, samt å skaffe seg en bedre forståelse av det fenomenet det dreier seg om.

I den banebrytende/tankevekkende artikkel «*Desperately Seeking the 'IT' in IT Research—A Call to Theorizing the IT Artifact*» hevder Orlikowski og Iacono (2000) at IS-forskningen ikke har vært opptatt av essensen i informasjonssystemene, dvs. de spesifikke egenskapene ved enkelte løsningene: «*its core subject matter—the information technology artifact*» (op. cit, p 1). Forfatterne skisserer et enkelt rammeverk for å klassifisere ulike perspektiver på IS i litteraturen. Deres kategorier «treffer» etter vår oppfatning ikke helt for å beskrive IKT-arkitektur; «ensemble-perspektivet»[4] synes å være det nærmeste kategorien. Vi argumenter for at et informasjonsinfrastruktur-perspektiv kan tilby en mer fruktbar innfallsvinkel til å analysere de ulike egenskapene ved en IKT-arkitekturer. Ikke minst kan dette perspektivet belyse en rekke av utfordringene som er knyttet til å innføre en bestemt IKT-arkitektur i forvaltningen, gjennom å forstå arkitekturen som komplekst «nettverk» av så vel tekniske og ikke-tekniske (organisatoriske, rettslige, institusjonelle osv) elementer, som derved også må håndteres ved ulike tilnærmingsmåter.

Nå vil kanskje ikke alle forstå det foreliggende forslag for IKT-arkitekturen som en selvstendig infrastruktur, fordi forslaget primært beskriver et rammeverk med en begrenset mengde tekniske komponenter. Disse skal imidlertid inngå i et sett av standarder, fellestjenester og støttefunksjoner, som samlet skal utgjøre en felles basis for forvaltningens eforvaltningsløsninger. IKT-arkitekturen vil berøre et mangfold av virksomheter, med egne IKT-løsninger (deriblant såkalte legacy systemer), ulike organisasjonskulturer og organisasjonspraksis, og ikke minst et omfattende regelverk. I informasjonsinfrastrukturteorien inngår dette i den *installerte basen*, som utgjøres av en forhistorie av tekniske så vel som ikke-tekniske elementer som infrastrukturen må tilpasse seg til. Som konkrete eksempel på slike ikke-tekniske elementer er rettsregler,

3 Se for eksempel. NOU 1978:48, som foreslår en del av de samme typer tiltak som den foreliggende FAOS-rapporten, men som ble avvist av Forbruker- og adm. Departementet i St.meld. 12 (1982-83).

4 Engelsk «ensemble view»: med underkategorier som «technology as Embedded System/» og Technology as Structure»

organisatorisk praksis i de enkelte virksomheter, betingelser knyttet til utvikling og bruk av løsninger osv.

Artikkelen vil derfor drøfte følgende forskningsspørsmål:

1. På hvilken måte er informasjonsinfrastrukturperspektivet relevant for arbeidet med en felles, offentlig IKT-arkitektur?
2. Hvordan skal vi forstå [begrepet] installert base for IKT-arkitekturen, og hvilke utfordringer representerer denne i arbeidet med å realisere IKT-arkitekturen?
3. Hvilke spesifikke egenskaper er viktig for informasjonsinfrastruktur for forvaltningen [til forskjell fra andre infrastrukturer]?
4. Hvilke konsekvenser vil det ha å legge et informasjonsinfrastrukturperspektiv til grunn for innføring av en felles IKT-arkitektur i forvaltningen?

Hensikten med artikkelen er å se i hvilken grad vi kan trekke på erfaringene fra tidligere arbeid med informasjonsinfrastrukturer. Vi vil også argumentere for at erfaringene fra arbeidet med felles IKT-arkitektur kan bidra til å berike teorien knyttet til informasjonsinfrastrukturer. Artikkelen har imidlertid ikke til hensikt å problematisere forslaget til en felles offentlig IKT-arkitektur som sådan.

Kort om den metodiske tilnærmingen

Denne studien baserer seg på et induktivt forskningsopplegg, hvor formålet er å bidra til en økt teoretisk forståelse av utfordringene knyttet til å utforme en felles IKT-arkitektur, og mer konkret hvilke krav en må stille til et slikt rammeverk som gjør det i stand til å understøtte brukerrettede eforvaltningsløsninger. Det teoretiske utgangspunket for arbeidet er elementer fra nettverksøkonomi og spesielt forståelse av informasjonsinfrastrukturer. Metodisk plasserer studien seg i hovedsak innefor kvalitativ tilnærming, med særlig basis i en fortolkende tradisjon innen IS-forskningen (Myers 1997: Myers and Avison 2002; Walsham 1993). Den empiriske basis for artikkelen bygger i stor grad på dokumentstudier, samtaler/intervjuer med sentrale aktører i arbeidet med å utforme en slik arkitektur. Konkret bygger analysene på rapporter og høringsuttalelser, samt flere åpne høringsmøter som har vært avholdt i dette arbeidet, og som har dannet bakgrunnsmateriale for departementets forslag til IKT-arkitektur[5].

Strukturen i artikkelen er som følger. I neste kapittel gis en kort presentasjon av den foreslåtte IKT-arkitekturen for offentlig sektor. Dernest presente-

5 Forfatterne har også på ulik måte vært involvert i dette arbeidet og vil nok trekke med seg egne synspunkter og erfaringer.

res artikkelens teoretiske basis, videre våre analyser knyttet til de enkelte forskningsspørsmålene, og avsluttes med en oppsummering av våre funn sammen med en kort drøfting av videre forskning.

2 Hva innebærer en felles IKT-arkitektur i offentlig sektor?

Tanken om en felles IKT-arkitektur i den norske forvaltningen ble først skissert i utredningen «Arkitektur for elektronisk samhandling i offentlig sektor» (Aad 2004)[6], og deretter presentert i St. mld. nr. 17 (2006-2007;s 120)[7], hvor det framheves at målsettingen for den felles offentlige IKT-arkitekturen er å få *«(...) ulike elektroniske system til både å passe og å arbeide godt saman»*. *Det forventes at resultatet av en velfungerende felles offentlig IKT-arkitektur kan «(...) bidra til betre brukarorientering og til meir effektiv offentleg ressursutnytting»* (ibid). Videre fremheves det at «(...) *gjennom å identifisere, strukturere og kategorisere element kan IKT-arkitektur både auke potensialet for gjenbruk på tvers, og redusere omfanget av unødig dobbelarbeid og slik redusere kostnader* (ibid). Den felles offentlige IKT-arkitekturen illustreres i figur 1[8]. Som det fremgår av figuren, består den foreslåtte arkitekturen av et presentasjonslag, et felleskomponentlag og et virksomhetslag. Ved å dele arkitekturen opp i flere lag som er uavhengige av hverandre antas den å bli mer endringsrobust ettersom endringer i ett lag ikke vil påvirke andre lag direkte. Intensjonen er at lagene skal sammenknyttes via standardiserte grensesnitt, og at åpne standarder er gjennomgående i alle lag. Presentasjonslaget er det grensesnittet borgere og næringslivet vil møte og få presentert tjenester fra offentlig sektor, eksempelvis MinSide, AltInn[9] eller virksomhetsspesifikke nettsteder. Det framheves at presentasjonslaget ikke framstår som «statisk» med ensidig fokus på presentasjon av tjenester gjennom portaler, men snarere at det tar høyde for å presentere tjenester også via ulike medier og kanaler, som Internett/PC'er, mobiltelefon, digital tv, osv. (Difi 2009).

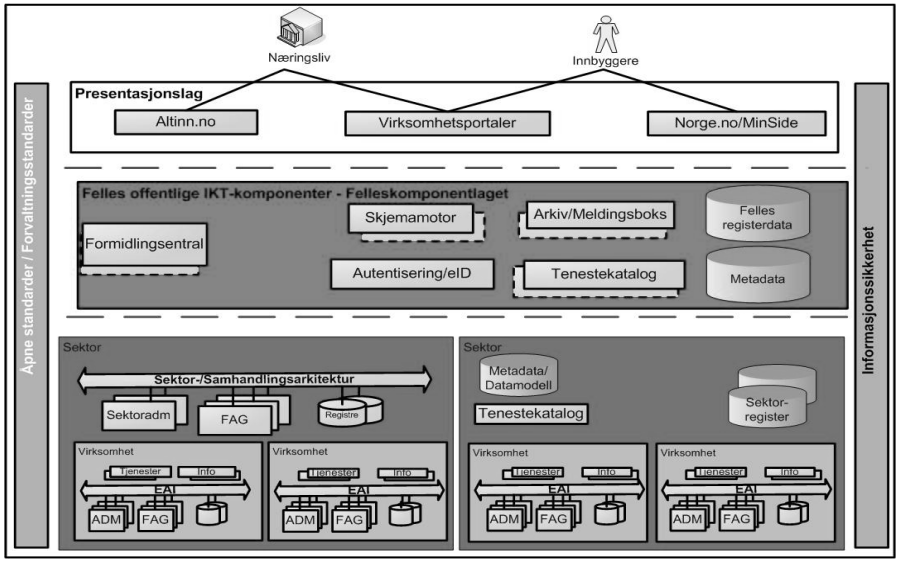
---

6 Utredningsarbeidet ble gjennomført av en arbeidsgruppe nedsatt av Arbeids- og administrasjonsdepartementet

7 Allerede da hadde en arbeidet med felles IKT-rammeverk i mange land, og det norske forslaget bygger i stor grad på arbeidet i Danmark, se f.eks. (Ministeriet for videnskab, teknologi og utvikling 2003).

8 Det understrekes at denne lagdelingen må betraktes som en logisk struktur som angir en arbeidsdeling, og ikke en beskrivelse av fysiske/tekniske lag som bygger på hverandre, som f. eks. protokoll-stakken i Internet.

9 Se www.altinn.no og www.MinSide.no



Figur 1: Felles arkitektur for IKT i offentlig sektor (Difi 2008)

I felleskomponentlaget vil det finnes komponenter som legger til rette for at offentlige virksomheter skal kunne utvikle elektroniske selvbetjeningsløsninger på et effektivt vis. Rasjonale er at offentlige virksomheter, til tross for at de arbeider på ulike virksomhetsområder og vil ha ulikt behov for IKT-løsninger, også vil ha sammenfallende behov på mange områder. Eksempelvis knytter dette seg til behovet for identifiserings- og autentiseringsløsninger, tilgang til grunndata, skjemamotor mv. Dermed anses det ikke formålstjenlig at hver virksomhet utvikler sine egne, spesialtilpassede løsninger for slike funksjoner, men gjenbruker eksisterende løsninger eller utvikler løsninger på en måte som gjør at de kan gjenbrukes av andre virksomheter. Det påpekes at dette laget er fleksibelt slik at det kan imøtekomme endringer etter hvert som nye behov oppstår, for eksempel ved endring, fjerning eller tilkomst av nye felleskomponenter. Vi vil senere i artikkelen vise hvordan en ved hjelp av lagdeling og modularisering kan oppnå slik fleksibilitet. Tjenestene som er angitt i denne figuren er å betrakte som eksempler og forutsetter at nye felleskomponenter kan innlemmes her etter hvert som behovet oppstår. IKT-arkitekturen bygger på 7 grunnleggende arkitekturprinsipper: tjenesteorientering, interoperabilitet, tilgjengelighet, sikkerhet, åpenhet, fleksibilitet og skalerbarhet (Difi 2009).

Virksomhetslaget representerer de enkelte virksomhetene og sektorene i forvaltningen, der de lokale arkitekturene, fagsystemene mv. finnes. Det er de

enkelte virksomhetene og sektorene som basert på felles arkitekturprinsipper, har ansvaret for å utvikle selvbetjeningsløsninger på sine respektive områder til borgerne og næringslivet. Både informasjonsinnholdet og den materielle logikken, dvs. regelverk som tjenestene bygger på, vil primært være den enkelte virksomhets ansvar. Når virksomhetene skal lage elektroniske selvbetjeningsløsninger, vil de benytte seg av egne komponenter, komponenter hos andre virksomheter, samt felleskomponentlaget.

I forslaget fra arbeidsgruppa påpekes det at IKT-arkitekturen i praksis ikke vil være et enhetlig og veldefinert byggverk (FAOS 2007). Den vil tvert i mot bestå av en rekke arkitekturer med tilhørende systemer, virksomhetsprosesser, standarder mv., representert ved mangfoldet av løsninger i virksomhetslaget. Derfor må arkitekturen i utgangspunktet forstås som et logisk rammeverk som danner grunnlaget for en videre utvikling og legger til rette for samordning av arkitekturene i de enkelte virksomhetene og sektorene, basert på en felles forståelse av hvordan disse skal utformes for å tjene fellesskapets interesser på en best mulig måte. Det må derfor skilles mellom overordnet IKT-arkitektur som et teoretisk rammeverk for hele forvaltningens IKT-løsninger, og de enkelte IKT-arkitekturer som faktisk eksisterer som konkrete sosio-tekniske konstruksjoner bestående av tekniske, organisatoriske og rettslige elementer som dessuten er under løpende utvikling i de enkelte etatene og sektorene[10]. IKT-arkitekturen i offentlig sektor kan betegnes som «national enterprise architecture» (NEA) (Janssen og Hjort-Madsen 2007) eller «government enterprise architecture» (Liimatainen 2008). En av flere definisjoner av enterprise architecture er «[…] *the organizing logic for business processes and IT infrastructure reflecting the integration and standardization requirements of the firm's operating model*» (Weill 2007). Janssen og Hjort-Madsen (2007) viser koblingen mellom enterprise architecure og national enterprise architecture ved at sistnevnte er basert på samme tenkemåte, men har offentlig sektor som sitt nedslagsfelt. Imidlertid blir det også reist kritikk mot denne tilnærmingen ved at den baserer seg på rasjonelt, teknologisk perspektiv (Ross, 2003), og at slike rammeverk ikke tar hensyn til at eksisterende institusjoner og etablert arbeidspraksis ofte er barrierer mot innføring av NEA, og likeledes at de er top-down orienterte (Janssen og Hjort-Madsen, 2007, p 2).

10 Her finnes store variasjoner i så vel statlig som kommunal forvaltning. Mens vi f eks. innen Skatteetaten, justissektoren finner enhetlige rammer for utvikling av nye eforvaltningsløsninger, er ikke dette et generelt trekk (Aad 2004), (FAOS, 2008).

3 Hvordan kan IKT-arkitektur forstås som en informasjonsinfrastruktur?

Det framheves i litteraturen at eForvaltning er et umodent forskningsområde, se f eks. Grønlund (2005), Grønlund & Andersson (2007), Heeks & Bailur (2007), Scholl (2009), og at IS-forskningen i liten grad har evnet å forstå mangfoldet og kompleksiteten i forvaltningen. Denne mangelen på teoretisk fundament synes å innebære at vi mangler et egnet begrepsapparat for å beskrive de ulike typer systemer og løsninger som den elektroniske forvaltningen baserer seg på. Som påpekt foran etterlyser Orlokowsi og Iaconi (2000) generelt en bedre forståelse (teoretisering) av de IKT-løsninger (IT artifacts) som studeres. Deres «ensemble view» kan gi fruktbare perspektiver, men favner ikke alle sider ved en IKT-arkitektur, blant annet installert base, som omtales nedenfor. Vi vil derfor søke å anvende informasjonsinfrastrukturperspektivet, da med den erkjennelse at det er ulike forståelser, som vi drøfter i det følgende.

Begrepet ble introdusert tidlig på 90-tallet, gjerne med referanse til Al Gore[11] sitt initiativ om å bygge et globalt informasjonsnettverk i USA. Sentrale bidragsytere i utviklingen av har vært Hanseth (1996), Hanseth og Monteiro (1996), Weill og Broadbent (1998). Som teori har den blitt brukt som basis for en rekke case-studier (Star and Ruhleder 1996; Ciborra 2000; Hanseth and Ciborra 2007). II-perspektivet har på ulike måter vist seg fruktbart innen IS-forskningen, både som beskrivelse av komplekse tekniske systemer (Ciborra 2000), og f. eks. knyttet til standardiseringsprosesser (Braa et al. 2007).

En kortfattet definisjon av informasjonsinfrastruktur er gitt av Hanseth og Lyytinen (2004: p 208): «*a shared, evolving, heterogeneous installed base of IT capabilities among a set of user communities based on open and/or standardized interfaces.*» Denne definisjonen innebærer at infrastrukturen skal være felles og kunne deles av alle relevante brukere, og at den vil være under løpende utvikling og tilpasning til sine omgivelser. Når vi sammenholder dette med prinsippene for IKT-arkitekturen, samsvarer dette med krav til tilgjengelighet, åpenhet, fleksibilitet og skalerbarhet, slik at den kan endres for å møte nye krav, og likeledes at den så langt mulig skal bygge på åpne standarder. Slik sett har IKT-arkitekturen sammenfallende egenskaper med en II, ved at den skal være tilgjengelig for et bredt spekter av brukere og interessenter, statlige og kommunale forvaltningsorganer og for IKT-leverandører til slike orga-

11 Al Gore brukte uttrykket *Global Information Infrastructure* på The first World Telecommunication Conference i 1994.

ner mv (Difi 2009).[12] I tillegg vil alle eforvaltningsløsninger måtte oppfylle de generelle krav som gjelder.[13] Den vil åpenbart være under løpende utvikling for å møte omskiftelige krav og behov som gjør seg gjeldende i omgivelsene, herunder politiske føringer, regelverksendringer, samt tekniske og funksjonelle elementer.

Star and Ruhleder (1996) presenterer imidlertid en annen tilnærming gjennom å hevde at

> *infrastructure is a fundamentally relational concept. It becomes infrastructure in relation to organized practices» (p. 4), og de sier videre: It is embedded into other structures, transparent in use, has reach and scope beyond a single event, is learned as part of a membership, it links with conventions of practice, embodies standards to be able to plug into other structures, is built on an installed base and, finally, it becomes visible upon breakdowns.*

Denne forståelsen vektlegger også andre dimensjoner, blant annet den sterke tilknytning til organisatorisk praksis og den skaper avhengighet hos sine brukere. Vi vil argumentere for at disse perspektiver er relevante i forhold til IKT-arkitekturen. Bygstad framholder tilsvarende at: «... it is fruitful to regard information infrastructure as an ICT-based organizational form.» Bygstad (2008, s 4).

Disse definisjonene viser ar det ikke er en entydig oppfatning av hva som forstås med en infrastruktur, men at de har fellestrekk som åpenhet (ikke lukket), standardisering, i stadig utvikling og at den bygger på en installert base. Slik sett samsvarer dette med målene og prinsippene for IKT-arkitekturen på et overordnet nivå. Vårt hovedpoeng er ikke at IKT-arkitekturen (i første omgang) skal forstås som en bestemt infrastruktur, men at infrastrukturperspektivet er relevant for arbeidet med IKT-arkitektur. Til forskjell fra generell teori om informasjonssystemer, legger informasjonsinfrastrukturperspektivet vekt på at man ikke vil ha enhetlige definerte brukergrupper, at man ikke har oversikt over hvilke endringer i krav og rammebetingelser som vil manifestere seg i fremtiden (Ciborra 2000, 2002). IKT-arkitekturen vil i praksis ikke vil være et enhetlig og veldefinert byggverk (FAOS 2007). Dette samsvarer godt med forståelsen av at IKT-arkitekturen vil omfatte en rekke arkitekturer med tilhø-

12 Det bør presiseres at pr. juli 2009 gjelder følgende (Difi 2009, s 8): Statlige virksomheter plikter å legge arkitekturprinsippene til grunn for IKT-prosjekter som fremmes som satsningsforslag i budsjettprosessen. Dette gjelder dersom forslagene gjelder utvikling av nye IKT-systemer eller vesentlig utvikling av eksisterende systemer [.]. For kommunal sektor er prinsippene anbefalte.

13 Dette omfatter blant viktige rettslige krav som knyttet til åpenhet, personvern og sikkerhet, videre arkivloven og universell utforming, krav til miljø osv.

rende lokale systemer, virksomhetsprosesser, standarder osv. For eksempel må ikke felleskomponentlaget oppfattes som den eneste kilden til komponenter, da en del komponenter vil tilbys direkte fra virksomhetene. Dette som illustrerer at det er mange involverte interessenter og at det dermed ikke vil være mulig for enkeltaktører å kontrollere arkitekturens utvikling. Helt sentralt er også at informasjonsinfrastrukturperspektivet, i motsetning til tradisjonelle IS-perspektiver, legger vekt på at det finnes en forhistorie av tekniske så vel som ikke-tekniske elementer, den installerte basen, som infrastrukturen må tilpasse seg til. Dette gir således en god indikasjon på at informasjonsinfrastrukturperspektivet er relevant og fruktbart for arbeidet med IKT-arkitektur.

Hva forstår vi med IKT-arkitekturens installerte base?

En sentral utfordring knyttet til å realisere IKT-arkitekturen er å beskrive og håndtere den installerte basen (Hanseth og Lyytinen 2004). Det er da nødvendig å forstå hva den installerte basen faktisk omfatter, og hvilke implikasjoner dette har for utviklingsarbeidet. Allerede i arkitektur-rapporten fra 2004 pekes det på en rekke bindinger til eksisterende, til dels leverandøruavhengige løsninger, gamle dataformater, samt en rekke lokale databaser og registre som er bestemt av ulike lover og forskrifter osv (Aad 2004, AFIN 2005). Dette er videre utdypet i FAOS-rapporten (FAOS 2007), og Riksrevisjonen peker i sin undersøkelse for eksempel på at mangelfull samordning av datadefinisjoner hindrer elektronisk informasjonsutveksling (Riksrevisjonen 2007, s 9). Med referanse til definisjonene foran vil vi med «*heterogeneous installed base*» forstå at IKT-arkitekturen bygger på en forhistorie av elementer bestående av tekniske, organisatoriske og rettslige komponenter, rutiner, arbeidspraksis og endog kulturelle og sosiale strukturer.

De tekniske elementene utgjøres av eksisterende løsninger og delsystemer, tidligere standarder for filformater, databaser og registre osv., som skal sikre samvirke mellom løsningene. I forvaltningen består disse elementene eksempelvis av en lang rekke IKT-systemer, både for oppgaveløsning internt i forvaltningen og for tjenesteyting overfor borgere og næringslivet. Slike IKT-systemer kan gjerne være basert på utdaterte standarder og løsninger, men som det er kostbart og tidkrevende å skifte ut (såkalte legacy-systemer). De fleste av disse systemene er utviklet innenfor den enkelte etat eller virksomhet, og kan være basert på særlover, som også gjerne omfatter legaldefinisjoner. Fordi mange slike legaldefinisjoner ikke er konsistente på tvers i lovgivningen[14], skaper dette

14 Typiske eksempler er «samboer»-begrepet, som er definert ulikt i minst 4 ulike lover (Schartum 2005b)

store problemer for samhandling på tvers. Det arbeides nå med ulike metadataregistre, for eksempel SERES. Et sentralt element er, som påpekt foran, at en installert base aldri er statisk eller «frosset», men at den vil utvikle seg i et dynamisk samspill med de ulike komponentene, og uten full styring eller kontroll av en sentral myndighet.

Rettslig regulering som en del av den installerte basen

De ikke-tekniske elementene i den installerte basen vil særlig være rettsregler som er felles for forvaltningen, eksempelvis forvaltningsloven, offentlighetsloven og arkivloven[15]. Regler kan fremstå som barrierer ved at lovregulering er vanskelig og tidkrevende å endre (politiske hensyn) eller at de er krevende å oppfylle, eksempelvis knyttet til personvern og informasjonssikkerhet, samtidig som det er et absolutt krav å ta hensyn til disse. Her kan det tenkes at IKT-arkitekturen kan bidra til å finne gode fellesløsninger, da ikke bare som tekniske felleskomponenter, men som «maler» for organisatoriske løsninger.

Det kan være ønskelig å avgrense vår forståelse av den «rettslige» delen av den installerte basen i forvaltningen til bare å inkludere de mest kritiske elementene. Dette vil imidlertid ikke alltid være mulig, da lover og forskrifter ikke uten videre kan oversees. Det primære er å forstå hvilke krav og bindinger som ligger fast på grunn av eksisterende lovgivning, til forskjell fra hva som er resultatet av tidligere praksis og som er uaktuelt i dag, og kanskje endog rettstridig fordi regelverket er endret.[16] Vi har foran argumentert for at en bør fokusere på å imøtekomme generelle lover, som allerede er reflektert gjennom eksisterende virksomhetsprosesser og IKT-løsninger. Øvrige rettslige reguleringer vil måtte innpasses etter hvert som løsningene som reflekterer dem blir aktuelle. Her vil en mulig strategi være å utvikle generelle minimumsløsninger som tilbys alle, og at den enkelte virksomhet vurderer behov for tillegg der dette er nødvendig. Dette kan skape større endringsfleksibilitet, også for å kunne innarbeide senere rettslige reguleringer. Slik sett vil en lettere kunne synliggjøre likheter og ulikheter, og kanskje endog på sikt redusere særegenhetene der dette ikke nødvendig for å ivareta politiske mål og prioriteringer, og kanskje gi anvisning på hvordan ulike krav skal oppfylles. Senere i artikkelen drøfter vi en strategi for dette.

15 Det presiseres at rettslige reguleringer først blir en del av den installerte basen når de er reflektert i for eksempel virksomhetsprosesser eller IKT-løsninger.

16 Jf f eks. ny offentleglov, og endringer i personopplysningsloven og forvaltningsloven

Hva slags type infrastruktur vil IKT-arkitekturen kunne utgjøre?

Ovenstående analyse synes å rettferdiggjøre at IKT-arkitekturen kan forstås som en generell eller generisk informasjonsinfrastruktur. Men den gir så langt ikke svar på hva slags type infrastruktur vi mer konkret snakker om. Hanseth og Lyytinen (2004) definerer tre vertikale kategorier: *universelle (Universal Service)* infrastrukturer som retter seg mot alle typer brukere og anvendelser. En slik universell infrastruktur bygger på et (flere) sett av internasjonale standarder for kommunikasjons og informasjonsutveksling. Internett er det mest typiske eksempelet, de globale telenettene er andre eksempler. Videre beskrives *bransjevise (Business sector)* infrastrukturer som vil rette seg mot avgrensede målgrupper, og tilby spesialiserte transaksjons- og datautvekslingstjenester, for eksempel finansnæringen, bilindustrien osv. Som en tredje kategori defineres *konsern (corporate)* infrastrukturer. Disse tilbyr informasjons- og transaksjonstjenester for sine interne brukere og andre samarbeidspartnere. Denne typen infrastrukturer er dermed mer avgrenset i sin innretning, og kan basere seg på standarder og tjenesteformer som er mer spesialiserte.

IKT-arkitekturen kan åpenbart ikke betraktes som en universell infrastruktur når det gjelder målgrupper og innretning, da den skal gjelde for en nasjonal forvaltning, i vår sammenheng den norske forvaltningen med sine spesifikke rammer og egenskaper. Vi vil også argumentere for at karakteristikkene som knyttes til en konserninfrastruktur heller ikke passer fullt ut for en slik felles IKT-arkitektur. Det er riktignok en del likhetstrekk knyttet til avgrensning og innretning, ved at det er mulig å fastlegge mer spesialiserte rammer og føringer, ikke minst hva gjelder styring og forvaltning. Men det er også forskjeller; blant annet fordi forvaltningen er politiker- og regelstyrt, og samtidig er forvaltningen, i det minste den norske, basert på bærende prinsipper om sektor- og linjeansvar. Budsjettprosessen, som har en horisont på ett år av gangen, gjør det også utfordrende å tenke langsiktig, særlig i statsforvaltningen. Det er derfor grunn til å hevde at forvaltningen er mer mangfoldig og vanskelige styrbar enn et konsern. En konserninfrastruktur vil også ofte basere seg på spesifikke interne standarder, som kan defineres uten hensyn til for eksempel åpen konkurranse eller spesifikt lovverk som sikrer åpenhet og generell tilgjengelighet.

I noen grad kan denne samsvare med en bransjeorientert infrastruktur, men samtidig har denne et mer avgrenset formål, funksjoner og bruksmåter. Vi vil derfor, i lys av argumentasjonen ovenfor, hevde at det kan være fruktbart å introdusere en egen kategori, *forvaltningsinfrastruktur,* som skiller seg fra både bransje- og konserninfrastrukturer både gjennom sin demokratiske innretning, med krav til åpenhet, rettsikkerhet og politiske styring, og de særegne prinsipper som gjelder for den politiske styringen som gjelder på ulike nivåer.

En første tilnærming er å forstå en *forvaltningsinfrastruktur* [17] som de tekniske, organisatoriske og rettslige strukturer som er nødvendig for at IKT-systemene i forvaltningen skal fungere etter hensikten. Dette samsvarer med Tilson og Lyytinen (2009, s 2), som definerer en infrastruktur som *«the basic physical and organizational structures needed for the operation of a society or enterprise»*. Her legges altså «normative» kriterier til grunn, i den forstand at definisjonen baserer seg på at oppsatte mål skal oppfylles. Særlig når vi ser på forvaltningen under ett, både den statlige og kommunale forvaltning, er det naturlig å betrakte disse som flere, adskilte infrastrukturer, både innenfor de enkelte sektorer/virksomheter og innenfor de ulike forvaltningsnivåer. Vi vil da forstå den felles *forvaltningsinfrastrukturen* som resultatet av en form for digital konvergens, beskrevet som «*an essential, pervasive and interactive reconfiguration of technical and social infrastructures of the whole government*». Dette må da forstås som en samling av felles elementer som vokser fram gjennom en evolusjonær harmonisering og sammenkobling av de ulike del-infrastrukturer, eller snarere de installerte basene som i dag finnes i forvaltningen. Imidlertid må denne definisjonen presiseres for å gi mening; vi må beskrive hvilke krav og rammebetingelser som gjelder i forvaltningen, hva de ulike [del]infrastrukturene består av, hvilke oppgaver/funksjoner de må oppfylle, og ikke minst hva konvergens innebærer konkret i denne sammenhengen, dvs. hvordan de ulike komponentene skal vokse sammen gjennom en gjensidig tilpasning. Sentrale rammer vil blant annet være: i) forvaltningens prinsipper som for eksempel sektorisering og linjeansvar, ii) en lovbestemt og politisk styrt arbeidsdeling mellom departementer og underliggende etater og virksomheter, iii) det [semi]-konstitusjonelle skillet mellom stat og kommune, iv) de grunnleggende rettslige rammer for offentlig virksomhet, som offentlighet, rettsikkerhet, personopplysningsvern[18] etc., v) krav til åpen konkurranse blant tilbydere til offentlige virksomheter, vi) krav til likestilling, universell utforming, miljøhensyn osv. og andre politiske og administrative føringer. Den foreslåtte IKT-arkitekturen utgjør således en del av et rammeverk som den framtidige forvaltningsinfrastrukturen skal utvikles innenfor, dels gjennom en overordnet planlagt prosess, men også ved mer eller mindre kontrollerte prosesser på ulike nivåer i forvaltningen.

En slik forvaltningsinfrastruktur vil ha mange fellestrekk med en bransje/sektorspesifikk infrastruktur, som også skal tilby spesifikke standarder og tje-

17 Denne konkretisering som er beskrevet her er knyttet til den spesifikke norske forvaltningen, men prinsippene vil kunne anvendes på en vilkårlig forvaltning.

18 Sentrale lover i denne sammenheng er offentleglova, forvaltningsloven, personopplysningsloven, arkivloven, lov om ikke-diskriminert og tilgjengelighet, som alle stiller spesielle krav til offentlige virksomheter

nester for samhandling og samarbeid innenfor sin avgrensede kontekst, hvor det vil være utformet egne regler og konvensjoner for datautveksling, forretningsmessig samhandling, generelle internasjonale standarder mv. Men det er også store forskjeller knyttet til styring og kontroll, standardiseringsprosesser osv. En bransjeinfrastruktur skal også legge til rette for lik, rettferdig konkurranse mellom mange av aktørene, mens andre hensyn gjelder for samvirke og arbeidsdeling mellom offentlige virksomheter, som mer er komplementære og i stor grad enerådende innenfor sine virkesområder, men samtidig politisk og administrativt styrt av Stortinget og regjeringen.

Slik sett er reguleringen og virkemidlene annerledes i forvaltningen enn både innen konserner og innen ulike bransjer eller sektorer i samfunnet. En konserninfrastruktur kan også framstå som mer enhetlig gjennom en samordning av ulike løsninger, fordi konserner vil ha andre virkemidler til å samordne disse uten å måtte ta hensyn til krav fra omverden på den samme måten som forvaltningen. Eksempelvis innførte Telenor på begynnelsen av 2000-tallet en ny styringsmodell for å sikre at konsernet, inkludert IT-systemene, skulle være i samsvar med sentrale krav og retningslinjer som kom i kjølvannet av Enron-skandalen og introduksjonen av nye revisjonskrav i Sarbanes-Oxley Act[19]. Resultatet ble en mer enhetlig portefølje av IT-systemer, samtidig som konsernet oppnådde sterkere styring av IT-utviklingen på de ulike forretningsområdene (Tversover 2007). Det er også noe av dette man ønsker å oppnå i forvaltningen, men man har altså ikke de samme virkemidlene for å gjennomføre det som i konserner og bransjer. Et konsern vil dessuten i større grad enn forvaltningen ha et felles mål og en samordnet strategi. Et ytterligere poeng knyttet til forskjellen mellom bransjer/konserner og forvaltningen er også at forvaltningen både er tjenestetilbyder og myndighetsutøver. En forvaltningsinfrastruktur skal både bidra til å tilby tjenester, styre og forvalte felles verdier og likeledes understøtte andre mål.

Vår definisjon illustrerer de åpenbare forskjellene mellom en forvaltningsinfrastruktur og en universell infrastruktur, særlig Internett, som primært er en transport- og service infrastruktur, både fordi målene og innretningen er forskjellig. Det synes derfor som om at erfaringene fra arbeidet med en universell, generell infrastruktur som f eks. Internett eller telenettet ikke alltid er like overførbare til arbeidet med IKT-arkitekturen. I nedenstående tabell søker vi å svare på hvilke spesifikke egenskaper som er sentrale for en informasjonsinfrastruktur for forvaltningen, til forskjell fra andre infrastrukturer.

19 Public Law 107 - 204 - Sarbanes-Oxley Act of 2002

Type II Krav/ virkemidler	Universell II, spesielt Internet	Bransje II	Konsern II	Forvaltnings II
Formål	Alle typer tjenester og bruksmåter	Tjenester og bruksmåter knyttet til en spesifikk bransje	Tjenester og bruksmåter innenfor et spesifikt konsern	Elektroniske tjenester til borgere og næringsliv, samt intern effektivisering i forvaltningen
Åpen og delt	For alle	Primært for aktører innen bransjen	Avgrenset til interne og samarbeidspartnere	Alle virksomheter i og leverandører til forvaltningen.
Dynamikk – hva er drivere?	Teknologi- og brukerdrevet	Drevet av brukerbehov og samfunnskrav	Forretningsdrevet	Både politisk styrt og virksomhetsorientert
Installert base	Eksisterende tekniske løsninger, som ble isolert eller minimalisert	Bransjespesifikke forhold, rettslig regulering	Interne tekniske og org. Forhold, relasjoner til omgivelsene	Rettsregler, politikk, forvaltningspraksis, legacy systemer osv
Brukere og bruksmåter	Alle typer brukere og bruksmåter	Bransjen og samarbeidende aktører	Interne brukere og samarbeids partnere, kunder	Borgere, næringsliv, forvaltningsorganer, politikere, organisasjoner, leverandører
Standardiseringsstrategi	Åpne prosesser hvor «alle» kan delta	Bransjeorientert	Interne prosesser	Åpne (demokratiske) prosesser, men politisk styrt
Styringsstrategi	Internasjonal konsensus	Bransjeorganer	Konsernstrategi	Politisk styring & forvaltningsprinsipper
Utviklingsstrategi	Faglig – evolusjonær, brukerforankret	Av representative aktører i bransjen	Forretningsdrevet	Sektor- og etatsbasert

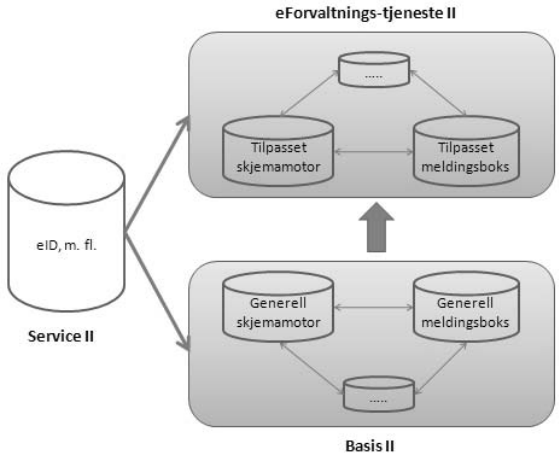
Denne oversikten viser at rammene for en forvaltningsinfrastruktur har en rekke fellestrekk med de andre kategoriene, men også sine særegne trekk, særlig knyttet til forvaltningsidealer og verdier som demokratisk styring, åpenhet og rettssikkerhet, i tillegg til sektor- og linjeansvarsprinsippene sammen med det kommunale selvstyret.

Noen konsekvenser av å legge et infrastrukturperspektiv til grunn

Ovenfor har vi vist at et informasjonsinfrastrukturperspektiv er relevant for arkitekturarbeidet. Dette innebærer også at erfaringer fra andre infrastrukturtiltak vil være nyttige for dette arbeidet. Nedenfor gis noen slike lærdommer, eksempelvis i forhold til modularisering og lagdeling for å oppnå fleksibilitet og bootstrapping for å sikre kritisk masse.

Horisontale infrastrukturer - modularisering og lagdeling

I forslaget til felles IKT-arkitektur er det foreslått en lagdelt struktur. Vi vil, i tråd med veletablerte prinsipper i objektorientert systemarkitektur, hevde at en forvaltningsinfrastruktur i utstrakt grad bør baseres på modularisering og lagdeling. Hanseth og Lyytinen (2004) illustrerer dette gjennom å vise at en infrastruktur kan deles opp i henholdsvis en applikasjons-infrastruktur og en underliggende støtte-infrastruktur, hvor sistnevnte igjen deles opp i en transport- og service-infrastruktur. En liknende tankegang om lagdeling av infrastrukturer kan være fruktbar å overføre til en forvaltningsinfrastruktur. Den vil da bestå av en *basis-infrastruktur*, en *eforvaltnings-tjenesteinfrastruktur* og en *service-infrastruktur*, se nedenstående figur 2. Basis-infrastrukturen vil inneholde generelle felleskomponenter, mens eforvaltnings-tjenesteinfrastrukturen vil inneholde spesialiserte felleskomponenter som bygger på de generelle. Eksempler på felleskomponenter som vil være del av basis-infrastrukturen kan være funksjonalitet for felles registerforvaltning og felles metadata, meldingsboks og skjemamotor. Dette innebærer at de generelle felleskomponentene i basis-infrastrukturen vil tilby et minimum av funksjonalitet som de fleste interessentene i IKT-arkitekturen finner nyttig og verdifullt. Funksjonalitet som ikke finnes i de generelle felleskomponentene vil deretter kunne realiseres av enkeltinteressenter ved å bygge på med spesialiserte felleskomponenter i eforvaltnings-tjenesteinfrastrukturen. Både de generelle og de spesialiserte felleskomponentene vil kunne benytte seg av felleskomponenter i service-infrastrukturen, for eksempel eID.



Figur 2: Lagdeling av infrastrukturer

I tillegg til å danne grunnlaget for elektroniske tjenester til borgere og næringsliv kan imidlertid også felleskomponenter tenkes brukt som gatewayer (oversettere eller sammenkoblere) ved å benytte standardiserte grensesnitt for å danne bindeledd mellom IKT-løsninger som i utgangspunktet er inkompatible, for eksempel av tekniske eller semantiske årsaker (Hornnes og Langeland, s 49).

Rettsregler som pådriver i forvaltningen.

Rettsregler kan sees på som en «pådriver», blant annet ved at nye rettsregler gir ekstra tyngde i innføring av nye løsninger. Den nye offentleglova med forskrift er et eksempel i så måte, ved at den pålegger alle departementene, samt statlige direktorater og tilsynsorganer med hele landet som virkeområde å gjøre postjournalene sine tilgjengelige for allmennheten på Internett via Offentlig Elektronisk Postjournal (OEP). I denne konteksten kan «bootstrapping»-strategi være relevant, ved at den rettslige reguleringen identifiserer og skaper et behov, men som det kan være krevende å få innført, blant annet på grunn av gamle systemer og praksis. Med bootstrapping menes «to promote or develop by initiative and effort with little or no assistance» (Hanseth & Aanestad 2002). Hanseth & Lyytinen (2004) fremhever her noen enkle prinsipper: i) design innledningsvis en tjeneste med utgangspunkt i nytte for utvalgte brukerne; ii) dra nytte av eksisterende installerte baser der dette er hensiktsmessig (men unngå andre deler av denne); iii) utvid eksisterende installert base ved å bruke en «overtalelses-taktikk» for å oppnå tilstrekkelig momentum (kritisk masse

av brukere; iv) lag løsningen så enkel og modulær som mulig, spesielt for å unngå en framtidig innlåsning til uheldig systemvalg.

Slike utvalgte brukergrupper bør være relativt avgrensede, slik at det er mulig å identifisere deres behov og samtidig representerer de en mer avgrenset installert base, som kan gjøre det mulig å innføre nye løsninger. Eksempelvis vil kundemassen hos Lånekassen kunne representere en slik avgrenset brukergruppe, som er godt motivert og har tilstrekkelige ferdigheter til å ta i bruk nye løsninger, f. eks. sikkerhetsløsningen i MinId og en felles meldingsboks. (Lånekassen 2008). Deres interesse ligger primært ikke i hele forvaltningsinfrastrukturen, de vil innledningsvis ikke se fordelene av hele IKT-arkitekturen. Men etter hvert vil deres bruk av en avgrenset del av denne kunne bidra til å øke verdien for hele infrastrukturen, jf. mekanismene i nettverksøkonomien som positive nettverkseksternaliteter. Tilsvarende mekanismer gjorde seg gjeldende ved introduksjon av første versjon av AltInn. I utgangspunktet ble denne utformet som en støtte til elektronisk innrapportering fra næringslivet til myndighetene, i første omgang begrenset til at løsningen kun omfattet tre etater og et begrenset sett med tjenester da den ble lansert, men den ble likevel oppfattet som nyttig blant målgruppene (AltInn 2006). Ved at det kun var med tre etater i starten var det mulig å få etablert løsningen raskere, i motsetning til om alle 22 etater som i dag er en del av løsningen skulle ha vært med fra starten av. I et forvaltningsperspektiv kan AltInn således være et eksempel på en minimumstilnærming, selv om vi ikke har grunnlag for å si om denne tilnærmingen var bevisst eller ikke.

Dette illustrerer at minimumsløsninger over tid gradvis kan videreutvikles og forandres i forhold til endringer i krav, rammer, forventninger mv. Dette forutsetter at IKT-løsningene er utformet slik at de er fleksible nok til å kunne endres etter at de er tatt i bruk. Hanseth og Lyytinen forklarer at denne fleksibiliteten har to perspektiver; *change og use* (2004). Forandringsperspektivet (change) handler om at en standard i informasjonsinfrastrukturen må kunne byttes ut med en annen, forbedret standard, uten at dette medfører store kostnader og usikkerhet. Bruksperspektivet (use) gir anvisning på at informasjonsinfrastrukturen skal kunne benyttes på ulike måter, og til ulike formål. Det gjøres også et poeng av at disse to perspektivene henger sammen ved at økt bruksfleksibilitet stiller mindre krav til forandringsfleksibilitet, og andre veien rundt. I praksis vil dette si at en IKT-arkitektur som er generelt utformet, vil ha mindre behov for å være fleksibel i forhold til forandringer enn en IKT-arkitektur som er mer spesielt og snevrere utformet.

Arkitekturarbeidet må derfor nettopp fokusere på hva de utvalgte brukergruppene ønsker seg av funksjonalitet, og sørge for å tilrettelegge for dette. Med andre ord fokuserer man på å gjøre arkitekturen attraktiv for dem ved hjelp av funksjonalitet, fremfor en omfattende installert base. Dersom det lykkes å lage

gode minimumsløsninger som bygger på installert base, vil det senere være mulig å dra nytte av nettopp nettverkseksternaliteter for å øke IKT-arkitekturens moment og omfanget av den installerte basen. Poenget er at nettverk, så vel fysiske som virtuelle, har økonomiske karakteristika i den forstand at verdien av å være tilknyttet dem øker med antallet andre som er tilknyttet. Eksempler på dette er blant annet fildelingsnettverk og sosiale nettverk som Facebook. En annen tjeneste som har slitt med å få oppslutning, er MinSide, som på grunn av begrensede tjenester ved introduksjon i 2007 skapte lite interesse og fikk derved negativ omtale. Nå er dette kanskje i ferd med å snu ved at MinId, autentiseringsløsningen i MinSide, nå benyttes i en rekke elektroniske tjenester fra det offentlige og således er mer utbredt og kjent blant befolkningen. Dessuten tilbyr mange kommuner nå sine tjenester gjennom MinSide.

Hvordan håndtere sektorisering og linjeansvarsprinsipper som en del av den installerte base.

En sentral del av forvaltningens installerte base er den eksisterende «silo-organisering», representert ved linjeansvars- og områdeprinsippet sammen med mål- og resultatstyring som da vektlegger den enkelte virksomhets resultatoppnåelse, hvilket også er det virksomhetene måles på av overordnet myndighet. Dette framstår som barrierer for gode e-forvaltningsløsninger ved at gevinster for fellesskapet ikke oppfattes som tilstrekkelig begrunnelse for nye, kostbare eforvaltningsløsninger. Dette reiser flere utfordringer, blant annet å sikre god utnyttelse av fellesløsninger på tvers av forvaltningen for de samme funksjonene, for eksempel økonomi, lønn/personal, arkiv osv. Det er derfor nødvendig å finne fram til mekanismer som kan sikre finansiering av utviklingskostnadene for felleslesning, men bruken av dem bør så langt som mulig være frivillig. Målet er å sikre at gode løsninger blir tatt i bruk fordi de framstår som nyttige og kostnadseffektive for de enkelte etatene og virksomhetene, og ikke gjennom overordnede pålegg («bruk av pisken»). Fokus er altså på en gulrot-strategi basert på kultivering, dvs. å legge til rette for en «organisk» utvikling gjennom at løsningene er generiske (Hanseth 2002, Ciborra 2002). Den økende bruk av Altinn kan stå som eksempel på denne tilnærmingen. Dette kan eksempelvis skje ved påvirkning gjennom faglig sterke enheter som ikke styrer ved hjelp av instruksjonsmyndighet, men indirekte ved hjelp av kompetanseheving, veiledning mv. På denne måten kan man bidra til at virksomhetene og etatene blir bevisste på nytten av fellesløsninger, samtidig som disse lettere kan tilpasses lokal praksis og organisering. Det sentrale her er at IKT-arkitekturen og fellesløsningene skal understøtte forvaltningens virksomhetsprosesser, og ikke at IKT-arkitekturen skal tres ned som en tvangstrøye.

Som påpekt foran har en også tidligere foreslått en rekke tiltak knyttet til samordning og fellesløsninger, hvor nettopp argumentasjonen har vært knyttet til sektor- og linjeansvarsprinsippene, jf. for eksempel NOU 1973:43, St.meld. 12 (1982-1983) og NOU 1978:48. NOU 1973:43 påpeker blant annet: *«[..] behovet for bedre samordning av arbeidet med planlegging og utvikling av edb-systemer, og spesielt forslag om en felles begreps- og systemstruktur og planleggingssystem»*. *Videre* slår Forbruker og administrasjonsdepartementet i St. meld. nr. 37 (1974-75) fast at «*ansvaret for administrativt utviklingsarbeid påligger primært den enkelte institusjon. Det bør derfor ikke gjennomføres sentrale, overordnede ordninger når det gjelder organisering av databehandlingen som medfører vesentlige endringer i dette forhold. Databehandlingsfunksjonene må vurderes som hjelpefunksjoner som det ikke kan være naturlig å ha en for sterkt sentralisert planlegging for.*» Mange vil i dag hevde at holdningen til ulike samordningstiltak er mer positiv, spesielt ut i fra den rolle IKT har i å modernisere forvaltningen, samt nødvendigheten av å bedre samarbeid på tvers for å kunne tilby bedre brukertjenester, jf Riksrevisjonen (2007). Likevel er det viktig å merke seg at St. meld. 19 (2008-2009)[20] vektlegger den enkelte etats selvstendig ansvar. Derfor må fellesløsninger og IKT-arkitekturen som sådan framstå som et positivt gode, og ikke noe som påtvinges virksomhetene.

En annen utfordring er å øke tilgangen til, og bruk av felles grunndata, dvs. sentrale registre og databaser i forvaltningen som tjener mange formål på tvers av etater og sektorer. Eksempler er Det sentrale folkeregisteret i Skattedirektoratet, eiendomsregistre og ikke minst de mange fellesregistrene i Brønnøysund-registrene (Olderbakk 2008). For noen av disse registrene er det både tekniske barrierer (manglende interoperabilitet), utilstrekkelig datakvalitet for andre enn de primære brukergrupper og også uhensiktmessige forretningsmodeller (Rasmussen Sørlie 2008). Det er nødvendig å forstå grunndata som en del av dagens installerte base som også vil utgjøre en [del]infrastruktur. Dette bør legges til grunn når en utvikler mer distribuerte modeller for forvaltning av slike felles ressurser som kan sikre tilstrekkelig god tilgjengelighet og datakvalitet samtidig som kostnadene fordeles på formålstjenlige måter. Regimene som er lagt til grunn for forvaltning av fri programvare kan eksempelvis være en inspirasjonskilde i denne sammenhengen.

Som allerede nevnt vil forvaltningsinfrastrukturens installerte base også bestå av «legacy-systemer». Disse systemene er ofte en viktig del av virksomhetenes fagsystemer, og kan ikke uten videre byttes ut over natten. Samtidig kan de

20 St. meld. 19 (2008-2009) Ei forvaltning for demokrati og fellesskap trekker opp hovedlinjene i forvaltningspolitikken og derved også premissene for IKT-politikken i staten.

være basert på utdaterte standarder og i tillegg være lite fleksible. Det faktum at disse systemene på den ene siden på noe vis må videreføres, og på den andre siden er lite fleksible, kan være en utfordring i forhold til en fortsatt evolusjon av forvaltningsinfrastrukturen. Bruk av gatewayer kan være fruktbart for å imøtekomme denne utfordringen. Slike gatewayer vil både kunne støtte «legacy-systemets» utdaterte standarder, samtidig som de vil støtte oppdaterte standarder, og således gjøre mulig å videreføre legacy-systemer som en del av den installerte basen, samtidig som det ikke begrenser forvaltningsinfrastrukturen evolusjon.

Konklusjon

I denne artikkelen har vi argumentert for at det kan være fruktbart å betrakte en IKT-arkitektur som en informasjonsinfrastruktur, og spesielt at det er nødvendig å forstå IKT-arkitekturens installerte base for å kunne håndtere denne på en konstruktiv måte, blant annet basert på begrepene bootstrapping og kultivering. Videre har vi definert en egen type infrastruktur, forvaltningsinfrastruktur, slik at vi kan synliggjøre både likheter og forskjeller mellom denne og andre typer infrastrukturer. Definisjonen kan bidra til å belyse forhold knyttet til utvikling, drift og vedlikehold av IKT-arkitekturen i et informasjonsinfrastrukturperspektiv. *Vi vil også framheve at Bygstads (2008) konklusjon om at «it is fruitful to regard information infrastructure as an ICT-based organizational form»* gir et viktig bidrag i å forstå hvilken rolle en IKT-arkitektur vil kunne spille i forvaltningen.

De konkrete drøftingene i denne artikkelen er basert på spesifikke egenskaper ved den norske forvaltningen, men tenkningen og prinsippene vil også kunne anvendes på tilsvarende arbeider innen andre nasjonale forvaltninger. Det er da nødvendig å forstå betydningen av den konkrete politiske, regulatoriske og organisatoriske kontekst som er definert av det enkelte lands konstitusjonelle rammer og forvaltningspraksis. Avslutningsvis vil vi trekke fram noen påstander som Orlikowski og Iacono (2000) presenterer i sin artikkel, og som vi mener har stor relevans for dette arbeidet

i. IT artifacts, by definition, are not natural, neutral, universal, or given. [..] Dette illustreres av at IKT-arkitekturene er ikke nøytrale, men at de er utformet med bestemte formål og underliggende interesser og normer, særlig knyttet til forvaltningspolitikken generelt, men spesielt til hvordan en ønsker å styre utviklingen av eforvaltningen i de enkelte land. Dette har således stor betydning for bruken og virkningene av IKT-arkitekturen.

ii. IT artifacts are always embedded in some time, place, discourse, and community. Dette samsvarer nettopp med vår vektlegging av en IKT-arkitektur, forstått som en informasjonsinfrastruktur, som er innbakt i en

konkret sosio-teknisk virkelighet gjennom forankring til en politisk, organisatorisk og institusjonell kontekst som ikke kan overses.

iii. *IT artifacts are usually made up of a multiplicity of often fragile and fragmentary components, whose interconnections are often partial and provisional and which require bridging, integration, and articulation in order for them to work together.* Dette samsvarer likeledes med vår forståelse av infrastruktur-perspektivet, og spesielt hvordan en forvaltningsinfrastruktur vil måtte bestå av en rekke del-arkitekturer med tilhørende systemer, virksomhetsprosesser, standarder mv. Disse vil være representert ved mangfoldet av løsninger i virksomhetslaget, som ikke vil være stabile over tid. Utfordringen er derfor å utforme et tilstrekkelig fleksibelt rammeverk som kan legge til rette for nødvendig samordning mellom de enkelte virksomhetene og sektorene.

iv. *IT artifacts are not static or unchanging, but dynamic*. Dette illustrerer at en forvaltningsinfrastruktur ikke kan forstås som ferdig eller fastlåst, men at den vil stadig tilpasse seg den omliggende organisatorisk og institusjonell praksis og vil endre seg over tid i samspill med sine omgivelser. Selv om løsninger framstår som ferdige og komplette, vil bruken av dem og virkningene endre seg over tid og dermed bidra til nye og uforutsette konsekvenser. Dermed må nye systemer som avløser de gamle må kunne integreres inn i infrastrukturen.

Referanser

Aad (2004) «Arkitektur for elektronisk samhandling i offentlig sektor». Arbeids – og administrasjonsdepartementet, se http //regjeringen.no/fad/

Braa, J., Hanseth, O., Mohammed, W., Heywood, A., and Shaw, V. «Developing Health Information Systems in Developing Countries. The Flexible Standards Strategy.,» *MIS Quarterly* (31:2) 2007, pp. 381-402).

Bygstad, Bendik (2008) Information infrastructure as organization. A critical realist view. *Twenty Ninth International Conference on Information Systems (ICIS 2008), Paris 2008*

Ciborra, Claudio (2000) A Critical review of the literature on the Management of Corporate Information Infrastructures. In Ciborra et al: *From control to drift*. Oxford University Press.

Ciborra, Claudio (2002): *The labyrinths of information. Challenging the wisdom of systems*. Oxford University Press

Edwards, P.N., Jackson, S.J., Bowker, G.C., and Knobel, C.P. Understanding Infrastructure: Dynamics, Tensions, and Design, 2007.

Grönlund, Å. (2005). State of the Art in E-Gov Research: Surveying Conference Publications, *International Journal of Electronic Government Research*, 1(4), pp. 1-25.

Grönlund, Å. and Andersson, A. (2006). e-Gov Research Quality Improvements Since 2003: More Rigor, but Research (Perhaps) Redefined, *Electronic Government*, LNCS 4084, pp. 1-12.

Heeks, R. and Bailur, S. (2007). Analyzing e-government research: Perspectives, philosophies, theories, methods, and practice, *Government Information Quarterly*, 24(2), pp. 243-265.

Hanseth, Ole & Kalle Lyytinen (2004): *Theorizing about the Design of Information Infrastructures: Design Kernel Theories and Principles*. Sprouts Working Papers on Information Systems. Tilgjengelig fra: http://sprouts.aisnet.org/124/1/040412.pdf

Hanseth, Ole & Margunn Aanestad (2001): *Bootstrapping networks, communities and infrastructures. On the evolution of ICT solutions in health care*. Tilgjengelig fra: http://heim.ifi.uio.no/~oleha/Publications/On%20the%20evolution%20of%20telemedicine%20networks4.pdf

Hanseth, Ole, Claudio Ciborra and Kristin Braa (2001) The Control Revolution. The EPR and the side effects of globalisation. *The Data Base for advances in Information Systems* 32(4) 34-46

Haraldsen, Arild (2003) *50 år - og bare begynnelsen* . Cappelen, Oslo

Jansen, Arild (2008): «Fra EMMA til Altinn». I: *Elektronisk forvaltning på norsk. Statlig og kommunal bruk av IKT*. Jansen og Schartum (red.) Bergen: Fagbokforlaget Vigmostad & Bjørke AS.

Janssen, Marijn og Kristian Hjort-Madsen (2007): *Analyzing enterprise architecture in national governments*. Proceedings of the 40th HICSS' 07. URL: http://www2.computer.org/portal/web/csdl/doi/10.1109/HICSS.2007.79

Liimatainen, Katja (2008): *Evaluating Benefits of Government Enterprise Architecture*. URL: http://www.iris31.se/papers/IRIS31-059.pdf

NOU 1978:48 Offentlig databehandling Desentralisering og effektivisering. Avgitt til Forbruker- og administrasjonsdepartementet

St.mld.12 (1982-1983) *Desentralisering og effektivisering i den offentlige databehandling og spørsmål om datapolitiske organer.* Forbruker- og administrasjonsdepartemenet

Ministeriet for videnskab, teknologi og utvikling (2003): *Hvidbok om IT-arkitektur*. Tilgjengelig fra: http://www.itst.dk/arkitektur-og-standarder/publikationer/arkitekturpublikationer/hvidbog-om-it-arkitektur/Hvidbog_om_IT-arkitektur.pdf

Myers, Mich., 1997 'Qualitative Research in Information Systems', MISQ Discovery, 2

Myers, Michael D. and David Avison (Eds.) 2002. Qualitative Research in Information Systems. London: Sage, 312 s. ISBN 0 7619 6632 3.

Olderbakk (2008). Utveksling av grunndata på personinformasjonsområdet. Juni 2007. Rapport til Finansdepartementet fra arbeidsgruppe, ledet av Håkon Olderbakk, BBREG. Tilgjengelig på http://www.regjeringen.no/upload/FIN/Vedlegg/sl/Rapporter/Persondatarapport%20%20-%2015%2006%202007.pdf

Orlikowski, Wanda J. and C. Suzanne Iacono (2001): Desperately Seeking the «IT» in IT Research—A Call to Theorizing the IT Artifact. Information Systems Research, _ 2001 INFORMS Vol. 12, No. 2, June 2001, pp. 121–134

Riksrevisjonen (2007) Riksrevisjonens undersøkelse av elektronisk informasjonsutveksling og tjenesteutvikling i offentleg sektor. Dokument nr. 3: 12 (2007-2008)

Schartum, Dag Wiese (2005b): *Utvikling av beslutningssystemer. Fra lovtekst til programkode*. Upublisert manuskript. Oslo: Avdeling for forvaltningsinformatikk. Tilgjengelig fra: http://www.jus.uio.no/ifp/afin/forskning/publikasjoner/notatserien/2005/utvikling_av_beslutningssystemer.pdf

Scholl, H.J. (200): Profiling the EG Research Community and Its Core. 1-12. In Wimmer et al (eds.): EGOV 2009, Linz, Proceedings. LNCS, 5693 Springer 2009, ISBN 978-3-642-03515-9

Star, S.L., and Ruhleder, K. «Steps Toward an Ecology of Infrastructure: Design and Access for Large Information Spaces» *Information Systems Research* (7:1) 1996, pp. 111-134.

St. mld. 37 (1974-75) *Om planleggingen av databehandlingen i staten* Forbruker- og administrasjonsdepartemenet

St.mld.12 (1982-1983) *Desentralisering og effektivisering i den offentlige databehandling og spørsmål om datapolitiske organer*. Forbruker- og administrasjonsdepartemenet

St.meld. nr. 17 (2006-2007). *Eit informasjonssamfunn for alle*. Fornyings- og administrasjonsdepartementet.

St.meld. nr. 19 (2008-2009): *Ei forvaltning for demokrati og fellesskap*. Fornyings- og administrasjonsdepartementet.

Tilson, D. og K. Lyytinen (2008) *Desperately seeking the infrastructure in IS research: Conceptualization of «Digital Convergence» as the co-evolution of social and technical infrastructures»*.

Walsham, G. (1993): Interpreting Information Systems in Organizations, Wiley, Chichester, 1993.

Weill, P., and Broadbent, M. Leveraging the New Infrastructure: How Market Leaders Capitalize on Information, Technology, Harvard Business School Press, Boston, 1998.

Weill, Peter (2007): *Innovating with information systems: what do the most agile firms in the world do?* The 6th E-business conference.

Internetthenvisninger

Difi (2009): *Overordnede IKT-arkitekturprinsipper for offentlig sektor*. Tilgjengelig fra: http://www.difi.no/IKT-arkitekturprinsipper_BHNq1.pdf.file

FAOS (2007): *Felles IKT-arkitektur i offentlig sektor.* Tilgjengelig fra: http://www.regjeringen.no/upload/FAD/Vedlegg/IKT-politikk/Felles_IKT_arkitektur_off_sektor.pdf

Lånekassen (2008): *Årsrapport 2007*. Tilgjengelig fra: http://www.lanekassen.no/upload/Arsrapport/2007/Lånekassens%20årsrapport%202007.pdf

Altinn (2006): Om Altinnsamarbeidet. Tilgjengelig fra: https://www.altinn.no/upload/3/OmAltinnforetater_sept06.pdf

Tversover (2007): IT-styring: *Referat fra PFIT-møte*. URL: http://www.espen.com/norskblogg/archives/2007/02/itstyring_refer.html [Lesedato 01.10.2009]3

THE NORWEGIAN DeCSS DECISION[1]

Jon Bing

1 Introduction

Professor Rik Kaspersen has become well known for his work on computer-related crime, not least for his leadership in the work of the Council of Europe ending with the Cybercime Convention.[2] Professor Kaspersen has also a tenuous family link to Norway, which is one of the reasons for the friendly relation to the Norwegian Research Center for Computers and Law. For this small paper, I have therefore tried to find a topic which combines these two aspects – computer-related crime and Norway. One possibility stands out – the criminal case against a Norwegian 15 years old lad for circumvention of the Content Scrambling protection system for movies stored on DVDs, using a program known as DeCSS. The case is known as the «DVD-Jon» case after the first name of the defendant, and is subject to comments in the international literature. DVD-Jon was acquitted, and the decision has been seen as a victory of the open source movement. This has elevated DVD-Jon from the ranks of ordinary hackers into a hero of the open source initiative.[3] It may be questioned if the decision of the court can be interpreted in such terms – the decision is rather more trivial. The Borgarting Appellate Court decision of 2003 may be found in an English translation at several sites on the net.[4]

2 The technical background and facts of the case

On the basis of a contractual arrangement between the largest movie companies in the USA and the DVD Copy Control Association Inc, there was developed a licensing scheme for movies marketed on compact disks. The compact disk could only be performed on players supporting the Content Scrambling

---

1 Published in *Caught in the Cyber Crime Act : opstellen aangeboden aan prof.mr. H.M.K. Kaspersen*/Arno Lodder, Anja Oskamp .- Kluwer, 2009, pp. 19-27.

2 Budapest 23 November 2001.

3 Robert Vaagan and Wallace Koehler «Intellectual propetrty rights vs. public access rights: ethical aspects of the DcCSS decryption program», *Information research* 3/2005 [http//information.net/ir/10-3/paper230.html].

4 See for instance http://www.ictlex.net/?p=61, the translation is by the author.

System, which was provided on the basis of a license contracted with DVD CCA. The licensee assigned one or two[5] «play keys» to the producer, which was to be protected. The play key is incorporated in the player, and had to be sufficiently protected against unauthorised access, otherwise the licensee according to the terms of the license agreement would have to pay a large penalty.

Using the play key the player may access the scrambler keys in the lead-in area of the compact disk. Using these, the stored movie can be unscrambled and performed.

The scrambling system is also used to maintain the zoning system which determines in which geographical area the movie is permitted to be performed. It also enforces the requirement that all players (or other devices performing movies) have to be licensed by the DVD CCA under the terms of the licensing agreement.

It is generally held that the encryption mechanism of CCS is weak. This is partly due to the legal restriction on encryption schemes in force in the USA at the time of the deployment of CCS which prohibited more than 40 bits encryption.

There is no doubt that unauthorised copying of movies represents a major problem. In the proceeding before the appellate court it was documented that the average cost for the production and marketing of a feature movie was 88 million US dollars, and only 20 per cent of the movies made a profit. For Warner Brothers, approximately 13 per cent of the income is generated from videocassettes, 47 per cent from compact disks.

In 1999 only illegal copying of compact disks which represented the problem. It was not seen as practical to copy movies from the Internet, in the appellate court decision, it is calculated that with the transfer rate of data available over an ISDN-line(8 GB) without compression, it would take 12 days to download a feature movie.

DVD-Jon was one of several waiting for the development of a player under the Linux operating system. During a couple of Internet Relay Chats in September 1999 he was told that the «nomad» had disclosed the code or the decryption algorithm in CSS. The «nomad» was supposed to have obtained this by reverse engineering of theprogram of the soft player Xing. The «nomad» had acquired the authentification code from the mail list LiVid (Linux Video) developed by Derek Fawcus.

5 The court notes that it has not ascertained the exact number of keys made available as the DVD CCA was not willing to reveal this, something maintained to be a trade secret.

The program developed by DVD-Jon was a graphical user interface integrating the decryption algorithm of the «nomad» and the authentification package of Derek Fawcus, designing the program for users without any special background knowledge. After testing the program on the move *Matrix,* DVD-Jon uploaded the program – DeCSS – to the Internet 6 October 1999. Over time, the program has been improved and made available in several different versions and under different operating systems (Windows 98 and Windows 2000). Curiously enough it was not made available under Linux, a program not used by DVD-Jon. It is claimed that this was due to Linux at this time not supporting the file format UDF.[6]

The DVD-CCA took legal action against several persons.[7] The Norwegian investigation started when the DVD CAA approached Økokrim, a central prosecution unit in Norway.[8] The case was tried by Oslo first instance court,[9] acquitting DVD-Jon. Økokrim appealed the case to Borgarting Appellate Court,[10] which also acquitted DVD-Jon, and which decision is discussed in this paper. The decision was not appealed to the Supreme Court.

3 The legal background

The major criminal provision, for which DVD-Jon was prosecuted, was the Criminal Code Sect 145(2). When Norway became independent from Denmark in 1814, the Constitution sect 94 required the parliament to legislate a «criminal law book». Such a general criminal act was adopted in 1902, and is still in force. Obviously, it is being constantly amended, the amendments being edited into the old statute.

The Criminal Code sect 145 is a time-honoured provision, penalising the unauthorised opening of a letter. Computer-related crime became a policy issue in 1978,[11] and already in 1979 the Criminal Code was amended. A major

6 Universal Disk Format, standardised by the Optical Storage Technology Association to form a common file system for all optical media.

7 Cf Allonn E Levy «DVD-litigation – Code on the Net» [http://www.legal.wao.com/decss.html], DeCSS Litigation Timeline [http://ipjustice.org/publications/decsstable.htm].

8 Økokrim is an acronym indicating that it is concerned with economic crime, computer-related crime has been organised within this specialist unit. There is no reason in this paper to dwell on the organisational features of the law enforcement in Norway, but it may be useful to note that there is integration between the police and prosecution – the highest ranking police officers are qualified as lawyers and appear as prosecutors in court for minor crimes.

9 Cf TOOSLO-2002-00507.

10 Cf LB-2003-00731.

11 The Norwegian Research Center for Computers and Law played an active role in bringing these issues of legal policy into the legislative agenda.

concern at that time was hacking, and there was no provision which directly addressed this in the Criminal Code. It was found that it could be appropriately regulated by including unauthorised access to computerised information in the venerable provision protecting the content of letters, in this way bridging the gap between new and old technology.[12] In 1987, a general revision with respect to computer-related crime resulted in an editorial amendment of the provision: it was given its own paragraph, and the wording was adjusted. It was qualified as a crime to «break a protection» for gaining unlawful access to «data or computer programs which are stored or are being communicated by electronic means». The term «data»[13] was explained in the government bill[14] to include all types of information «for instance on personal, technical or economical issues. The term should be interpreted broadly.» Indeed, the term was thought to be *too* broad, it would – the legal history indicated – also include television signals, which might be scrambled to ensure that only subscribers, who were provided with a smartcard for descrambling the signal. The penalty of section 145(2) was seen as excessive for unlawful circumventing a television scrambling system, and a special provision was proposed for this. However, the Parliament did not pass this special provision,[15] and only the amended the Criminal Code section 145(2).

One should note that the provision qualifies *unlawful* access by breaking a protection as the relevant criterion. Whether the access is unlawful, is not decided by sect 145(2), but by other provisions. Discussing «unlawful», the government bill gives as example a cleaner accessing the computer system in the company he or she is employed. «In general, the requirement that the act is unlawful must be interpreted as a general reservation primarily referring to norms outside criminal law».

This was the state of the Criminal Code at the time the case of DVD-Jon was tried. Later, sect 145(2) has been amended once more.[16] The reference to «breaking a protection» has been removed, and the provision is now qualifying «unlawful access to data» as a crime. However, a number of other amendments were made at the same time to implement the Cybercrime Convention, for instance making passwords available *etc*.

12 Cf Ot prp no 4 (1978-1979), the Government bill to the Parliament.
13 Which is also the term used in Norwegian.
14 Cf the government bill, Ot.prp no 35 (1986-1987). Under Norwegian law, the legal history is a major source for interpreting the statute, often the statutory text is rather brief, leaving to the legal history to explain how to interpret and apply the provisions.
15 However, in 1995 a similar provision was included in the Criminal Code as sect 262.
16 Act of Parliament 2005:16.

One should perhaps remind the reader that the case was tried before the Copyright Directive[17] was passed, and before its provisions on Digital Rights Management were implemented in Norwegian law.

4 The decision

There was little disagreement about the facts of the case. Most of the discussion was on the application of the Criminal Code sect 145(2).

Under Norwegian law, the interpretation of criminal law is strict, in the sense that the words are to be interpreted as understood by a general user of Norwegian, not as legal or technical terms. This is based on the Constitutions sect 96 which requires statutory authority as the basis of a criminal judgement. This is in contrast to the doctrine for civil law, where a court may base its decision on general and unwritten principles of law, making Norwegian law somewhat different from the typical Continental European law.

In making the decision, there are four major points on which the court has to make a decision.

4.1 «Data»

The appellate court first had to decide whether the movies which the defendant accessed, were to be qualified as «data» as the term was used in the Criminal Code sect 145(2). One may initially see this as a rather straightforward issue, but a couple of older Supreme Court decisions made this less obvious.

The decisions related to the use of a pirate decoding smartcard for scrambled television. The purchaser of such a card would insert it into the set-top box, and the television signal would be unscrambled. The issue before the Supreme Court was whether this could be qualified as breaking a protection to unlawfully gain access to data. It was found that a protection was broken, and that it was unlawful as the purchaser had not paid the access fee to the cable television company. It has been mentioned above that a similar situation is discussed in the legal history, where it was stated that the Criminal Code sect 145(2) in principle applied, therefore an alternative section had been proposed for this situation, a proposal not accepted by the Parliament. One should therefore think that it was rather obvious that the television programs were «data». But the Supreme Court held that «data» should be interpreted as «the communication of computerised information for payment», and that this

17 Directive of the European Parliament and of the Council on the harmonisation of certain aspects of copyright and related rights in the information society, direktiv 2001/29/EC.

«on the basis of common understanding is something different from television programs».[18] This interpretation of the Criminal Code sect 145(2) was confirmed by a second Supreme Court decision.[19]

The movies stored on a DVD would be rather similar to a television program. It was therefore by no means obvious that such movies would be qualified as «data» according to the Criminal Code sect 145(2). But the appellate court does not elaborate this point, rather the court finds it «beyond doubt» that the movies represent «data» in the understanding of the Criminal Code sect 145(2).

There has been, in the international discussion of the case, expressed some curiosity why the prosecution decided to bring a case against a young person before the court, as the defendant hardly was a typical criminal, and easily would win the sympathy of the public (as indeed he did). The author suggests that one explanation is this rather technical, legal point. The major provision applying to hacking was the Criminal Code sect 145(2), but its area of application was brought into doubt by the two unhappy decisions by the Supreme Court relating to pay-TV. Through the case against DVD-Jon the prosecution wanted to determine the application of the provision to computerised entertainment systems, containing the damage of the two Supreme Court decisions on the interpretation of «data» as a general term. Though DVD-Jon was acquitted, the prosecution obtained the consent of the appellate court to the broad interpretation of «data».

4.2 «Unlawful» – copyright infringement

In order to apply the Criminal Code sect 145(2), the act of the defendant has to be «unlawful». As explained in the legal history, whether an act is unlawful will typically be determined by norms outside the Criminal Code.

It should perhaps be emphasised that the Criminal Code sect 145(2) is a protection against the unlawful access to data. It does not make the breaking of protection mechanisms criminal as such. There are examples of such provisions; for instance the protection of technological measures provided by the Copyright Directive sect 6 protects against the circumvention of technical measures as such. But the Criminal Code sect 145(2) can only be applied when demonstrated that the breaking of the protection result in an unlawful access of information.

18 Cf HR-1994-179-B.
19 Cf HR-1995-2-A.

The obvious alternative would be copyright infringement. In the context of the Internet, there is no lack of examples of illegal uploading or file-sharing. Above, it is explained that at the speeds of Internet lines available at the time of the case, it was impractical to download movies.

The DeCSS program would not only permit the performance of the movie, it would also make it possible to copy the movie to a hard drive, and from this it would be possible to reproduce the movie on other storage media (though the burning of DVDs was not trivial at this time).

It could not be demonstrated that the defendant had accessed other movies than those he himself had purchased. Under the Norwegian Copyright Act Sect 12, it is permitted to reproduce copies for private use.[20] Therefore, decrypting the movie for storing a copy for private use would not be a copyright infringement, and not an unlawful act.

It was maintained that the label «DVD» on the cover implied a limitation of the default permission to make reproductions for private use. Norwegian law will give priority to a contractual arrangement between the parties to limit the default permissions in the Copyright Act, but unilateral statements are not generally accepted as binding. The court makes reference to one of the earliest government reports on computerisation and copyright,[21] this report discusses the practice of shrink-wrap licenses for computer programs, but the point is of a general nature.

Consequently, it could not be demonstrated that the acts of the defendant were copyright infringement.

4.3 Unlawful – reverse engineering

Above has been mentioned that the defendent for the DeCSS used a program made available from the «nomad». It was maintained that this program had been reverse engineered by the «nomad» on the basis of the program of a Xing player. The court points out that the developer of a program is permitted to establish compatibility through reverse engineering. The court also states that the program philosophy of the open source movement would make it impossible to accept the license terms of the DVD CCA. If a player for the operative system Linux was to be developed, reverse engineering was – the court seems to imply – the only alternative left to the developer, in this case the «nomad».

However, little is known about the «nomad» and the development of the program. It is not known whether all the requirement of the provision permit-

20 Cf also Copyright Directive sect 5(2)(b).
21 Cf NOU 1983:35.

ting reverse engineering were satisfied, for instance whether the «nomad» had lawful access to the Xing program. It was not certain that only the parts of the program necessary to establish functional interaction had been reverse engineered. Also, it is suggested that the «nomad» was German, and the reverse engineering had taken place in Germany and (probably) governed by German law. Though copyright law is co-ordinated both by the Berne Convention and European directives, there should in principle be determined whether the reverse engineering was permissible under the *lex causae*. The appellate court uses the failure of the prosecution to secure evidence relating to the «nomad» and the reverse engineering to apply the rules on the burden of proof, finding it not proven that the decompilaton of the «nomad» was illegal.

Furthermore, the court holds that it hardly can be required by a youth of 15 years to be familiar with the provisions on reverse engineering in the Copyright Act. The court did not find accessing the play keys as such illegal – the court held that play keys did not enjoy any protection themselves, the question of whether the act was unlawful, had to be decided with respect to accessing the movie stored on the compact disk.

4.4 Unlawful – contributory infringement

In the case, it could not be proven that the defendent had infringed the copyright of any movie. But it is rather obvious that DeCSS could be – and would be – used for such purposes. When the program was uploaded to the Internet, it could be downloaded by persons who use the program for reproducing copyrighted movies beyond what were permitted by the provisions on private copying or other exceptions to the exclusive right justified.

The court therefore discussed whether this potential would make the breaking of the code unlawful. The reasoning was that making DeCSS available might be a contribution to copyright infringement by third parties; this would make the defendant liable for contribution towards copyright infringement, and would also make the development of DeCSS unlawful.

The court cites a major authority on criminal law: «Almost anything can be used for committing a crime. Some objects even imply the possibility for illegal use. But it is the unanimous view that criminal liability in such cases is excluded both for producer and seller.»[22] The possibility for DeCSS to be used for copyright infringement – even the *probability* of such infringing use – was not sufficient to establish criminal liability for the defendant. And, the courts

22 The monograph is Erling Johannes Husabø *Straffeabsvarets pereferi* Bergen1999:100.

emphasis, the prosecutor has failed to give as much as one example of DeCSS actually having been used for copyright infringement.

5 Acquitting DVD-Jon and conclusions of the case

The court did not find that the breaking of the code to access or make a copy for private use of the movie on the DVD purchased by DVD-Jon presented an *unlawful* act. Therefore, the Criminal Code sect 145(2) could not be applied, and DVD-Jon was acquitted.

In considering the arguments as sketched above, one will appreciate that the case is perhaps more about copyright than criminal law. The prosecution was successful in proving that DVD-Jon did break a protection to access the data in the form of the movies stored on a compact disk. Actually, this was not really in question, to a large extent this was admitted by the defendant himself.

What is left is the requirement that such an act has to be «unlawful» – *ie* that accessing the data was contrary to law. Such law have to be found outside the criminal provisions; it is a reference in general to the rules governing our actions. There may be several reasons why accessing information is illegal – as mentioned above, in the legal history is mentioned a cleaner accessing the computer system of his or her employer, which would be contrary to the norms governing the employment contract.

One of the alternatives discussed in the court decision is whether the reverse engineering – which was the basis of the program developed by the «nomad» for decryption of the compact disk. The arguments that reverse engineering were permitted because the «nomad» could not accept the terms under which a license was offered, is not convincing. It cannot be sufficient for triggering the provision on reverse engineering that the beneficiary finds that the terms on which information for functional interaction is offered, are not acceptable. It cannot be excluded that the terms have to be qualified as prohibitive, and therefore equal to denying access to the information. But this obviously cannot rely on the assessment of the beneficiary alone. The court would have to argue this point in order to have a satisfactory justification. As it is, the court glosses over this problem. It is difficult to see that the development of the program by the «nomad» could be lawful under the co-ordinated European law on reverse engineering.[23] The court also seem to be willing to make the legal ignorance of this by the 15 year old DVD-Jon relevant, but it would again seem difficult to justify such a view – even if the ignorance was taken into consideration, the act

23 Council directive of 14 May 1991 on the legal protection of computer programs (91/250/EEC) art 6.

could not be qualified as lawful, though criminal liability might be excluded for this reason.

However, it must be admitted that the issue of the lawfulness of the reverse engineering of the program developed by the «nomad» is rather technical. It is probably governed by German law, and the prosecution had failed to secure evidence to satisfy the court. The court obviously is reluctant to decide the case on this somewhat obscure issue. But it would seem to the author that the program of «nomad» could not have been lawfully decompiled, and consequently the program itself was either an unlawful reproduction of the protected program,[24] or it utilised knowledge obtained by unlawful means. This would make DeCSS unlawful, and would have justified the application of the Criminal Code 145(2).

Another issue is the construction of the access to data. Obviously, the objective was to gain access to a movie. But in order to have access to the move, a key had to be retrieved from those stored on the compact disk. The player matched its play key to the stored keys, and would then decrypt the movie. The court considers the access to the stored keys as auxiliary to accessing the movie, and does not discuss this as a separate act. The court maintains that the keys are not protected – and certainly they are not protected by copyright. But there is the possibility under European law that the collection of keys on the compact disk is a small database, and that the access is an infringement of the *sui generis* database right.[25] It is perhaps understandable that the court does not choose to apply – or even discuss – this alternative; it would again be rather technical and perhaps difficult to explain.

The case has been presented in the international commentaries as a victory for the open source movement or similar policies. As the discussion above discloses, it really is a decision on what is protected by the provision of criminal law in question. This provision does *not* protect encryption schemes or technical measures. Breaking such a protection was one of the necessary criteria to be met on applying the provision, and there was no disagreement that the defendant had broken a protection measure. But this was not the major criterion – the act also had to be «unlawful», which was decided by legal rules external to the criminal law. As was briefly indicated in the introduction, developments after the case have removed the criterion of breaking a protection from this provision. What today remains is a prohibition of unlawful access to

24 The appellate court seems to consider the program developed on the basis of the reverse engineering not a reproduction (in copyright terms) of the program subject to decompilation.

25 Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases.

information in computerised systems. In addition, there are now other provisions addressing compromising security measures, like gaining knowledge of another person's password, *etc*.

However, the case has made a name for DVD-Jon, and perhaps made s small contribution to better understanding the nature of computer-related crime.

KOMMUNER OG INFORMASJONSSIKKERHET. ETTERLEVELSE AV KRAVENE I PERSONOPPLYSNINGSLOVEN OG FORSKRIFTEN[1]

Tommy Tranvik

Innledning

Personopplysningsloven og forskriften inneholder bestemmelser om informasjonssikkerhet. Disse finnes i lovens § 13 og i forskriftens kapittel 2.[2] Her pålegges de behandlingsansvarlige (de som bestemmer formålet med behandlingen av personopplysningene[3] og hvilke virkemidler som benyttes) å iverksette «systematiske og planlagte» sikringstiltak.[4] Formålet med tiltakene er å gi enkeltpersoner tilfredsstillende beskyttelse mot krenkelser av grunnleggende personvernhensyn, spesielt privatlivets fred og den personlige integriteten, som kan oppstå når behandlingen av opplysningene helt eller delvis skjer ved hjelp av elektroniske hjelpemidler.[5] De behandlingsansvarlige skal derfor sørge for at personopplysningene er beskyttet mot tre typer sikkerhetsbrudd:

---

1 Denne artikkelen springer ut av forskningsprosjektet *Legal Information Security Regulations: An Instrumental Perspective* utført ved Avdeling for Forvaltningsinformatikk, Universitetet i Oslo. Prosjektet er finansiert av Norges Forskningsråd over programmet *IKT, sikkerhet og sårbarhet*.

2 Reglene om informasjonssikkerhet i personopplysningsloven og forskriften er basert på Den internasjonale standardiseringsorganisasjonens anbefalinger (med utgangspunkt i standarden ISO/IEC 17799 2005 som i 2007 ble videreført i ISO/IEC 27002 2005).

3 Personopplysninger defineres som opplysninger eller vurderinger som kan knyttes til fysiske personer: alt fra kontaktinformasjon – navn, adresse og telefonnummer – via fødselsnummer og informasjon om fritidssysler, livssyn eller sosiale forhold til konto- og helseopplysninger (jf. personopplysningsloven § 2).

4 Det dreier seg om fire hovedtyper tiltak: organisatoriske, teknologiske, bygningstekniske og personalmessige. Organisatoriske tiltak omfatter bl.a. etablering av en sikkerhetsorganisasjon (hvor myndighet, ansvar og arbeidsoppgaver fordeles), mens brannmurer, krypteringsløsninger, antivirusprogrammer, spamfiltre og teknisk tilgangsstyring er eksempler på teknologiske tiltak. Bygningstekniske tiltak inkluderer inndeling av bygninger i ulike soner (og kontroll med hvem som har tilgang til dem), og personalmessige handler i hovedsak om å styrke de ansattes sikkerhetskompetanse.

5 Jf. personopplysningsloven §§ 1 og 3.

- Konfidensialitetsbrudd: personopplysningene blir gjort kjent for andre enn de som har tjenestelige behov for tilgang til dem.
- Integritetsbrudd: personopplysningene endres (eller manipuleres) av andre enn de som har fullmakt til å foreta endringer.
- Tilgjengelighetsbrudd: personopplysningene er utilgjengelige for de som har tjenestelige behov for tilgang til dem.

For å oppnå tilfredsstillende informasjonssikkerhet kreves det at sikkerhetsarbeidet baseres på prinsippet om risikostyring. Risikostyrt sikkerhetsarbeid innebærer at potensielle og uakseptable sårbarheter/trusler mot personopplysningenes konfidensialitet, integritet og tilgjengelighet skal forutses og reduseres (til et akseptabelt nivå) før alvorlige sikkerhetsbrudd inntreffer. Risikostyring innebærer også at det stilles en rekke krav til organiseringen og gjennomføringen av sikkerhetsarbeidet:[6]

- Det skal etablere et internt ledelsessystem – en sikkerhetsorganisasjon – for å ivareta informasjonssikkerheten.
- Den daglige ledelsen i virksomheten har ansvaret for at bestemmelsene om informasjonssikkerhet i personopplysningsloven og forskriften overholdes og at sikkerheten er tilfredsstillende.
- Risikoen for sikkerhetsbrudd skal ikke elimineres – det er ikke snakk om nulltoleranse – men sikkerheten skal være tilfredsstillende.
- Den behandlingsansvarlige skal selv avgjøre hva som menes med tilfredsstillende informasjonssikkerhet («hva er god nok sikkerhet her hos oss?»).
- Risikovurderinger skal benyttes for å identifisere potensielle og uakseptable sårbarheter/trusler mot informasjonssikkerheten.[7]
- Det skal iverksettes sikringstiltak slik at uakseptable sårbarheter/trusler reduseres til et akseptabelt (eller tilfredsstillende) nivå.

---

6 For nærmere diskusjoner av risikostyring og organisering av informasjonssikringsarbeidet, se for eksempel Slay og Koronios 2006, Daler et al. 2002: 121-142, Schneier 2000: 301-302 eller Saltmarsh og Brown 1983. For diskusjoner av informasjonssikkerhet og personvern i et rettslig perspektiv, se for eksempel Seipel 2006, Schartum 2005 eller Johansen et al. 2001: 128-133 og 344-357.

7 Trusler/sårbarheter identifiseres og sikringstiltak iverksettes på bakgrunn av risikovurderinger. Ved risikovurderinger stilles og besvares to spørsmål: (1) hvor stor er sannsynligheten for at ulike typer trusler/sårbarheter fører til sikkerhetsbrudd og (2) hvor alvorlige krenkelser av den enkeltes personvern kan potensielle sikkerhetsbrudd innebære? (se personopplysningsforskriften § 2-1). Problemet er at både sannsynligheten for og de personvernmessige konsekvensene av sikkerhetsbrudd kan være ukjent. I slike tilfeller er uvitenheten (om sannsynlighet og konsekvens) så stor at det blir vanskelig å fatte risikobeslutninger (se for eksempel Collingridge 1980: 23-32), og det kan tenkes at beslutningene like gjerne baserer seg på «frimodig gjettverk» som på «rasjonelle analyser».

- Den behandlingsansvarlige skal selv avgjøre hvilke sikringstiltak som bør iverksettes og kontrollere at tiltakene gir den ønskede sikkerheten.

Samtidig inneholder personopplysningen og forskriften omfattende krav til sikkerhetsdokumentasjon. For det første skal iverksatte sikkerhetstiltak dokumenteres. For det andre skal sikkerhetsbrudd (og forsøk på sikkerhetsbrudd) dokumenteres. For det tredje skal det interne ledelsessystemet for informasjonssikkerhet dokumenteres. Denne siste typen dokumenter omfatter beskrivelser av sikkerhetsorganisasjonen, sikkerhetsmål, sikkerhetsstrategi, oversikt over informasjonssystemenes utforming og overordnede retningslinjer for sikkerhetsarbeidet (for eksempel opplegg for gjennomføring av risikovurderinger, rutiner for ledelsesgjennomganger, rutiner for avviksmelding og rutiner for gjennomføring av sikkerhetsrevisjoner).

Nedenfor diskuteres hvordan 19 kommuner på østlandsområdet (a) overholder kravene til organisering og gjennomføring av sikkerhetsarbeidet og (b) overholder kravene til dokumentasjon av det interne ledelsessystemet for informasjonssikring (styrende dokumenter).[8] Argumentet i artikkelen er tredelt. For det første at kommunene i studien står overfor store utfordringer når det gjelder å etterleve kravene til organisering og gjennomføring av sikkerhetsarbeidet. For det andre at de (i stor grad) overholder kravene til utarbeidelse av styrende dokumenter. For det tredje at beskrivelsene av sikkerhetsarbeidet som gis i de styrende dokumentene ikke stemmer med hva som faktisk gjøres. Dermed oppstår det som kan betegnes som en etterlevelsesillusjon: dokumen-

8 To av kommunene i studien er mellomstore (begge med omkring 18 000 innbyggere), mens resten er store kommuner (20 000 eller flere innbyggere). Kommunene fordeler seg på seks fylker: Oppland, Hedmark, Akershus, Buskerud, Vestfold og Østfold. De operativt ansvarlige for informasjonssikringsarbeidet (sikkerhetsledere) og IKT-sjefer i hver kommune ble intervjuet. I noen tilfeller ble også rådmenn/assisterende rådmenn intervjuet. I tillegg ble kommunale personvernombud intervjuet der hvor det fantes. Hensikten med intervjuene var å kartlegge erfaringene til de som til daglig jobbet med å etterleve reglene, og spørsmålene som ble stilt baserte seg på bestemmelsene i personopplysningsforskriftens kapittel 2. Samtidig ble det innhentet data i form av dokumenter som beskrev kommunenes arbeid med regeletterleve. På nasjonalt nivå ble ledere og ansatte i Datatilsynet intervjuet. Alle stedlige kontrollsaker i kommunesektoren ble gjennomgått for hele perioden etter at personopplysningsloven og forskriften trådte i kraft, det vil si fra 1. januar 2001 til utgangen av 2008 (her dreier det seg om 85 stedlige kontroller). Andre dokumenter – Datatilsynets årsmeldinger, interne strategier og policydokumenter, informasjons- og veiledningsmateriale, lov- og forskriftskommentarer, høringsuttalelser, kampanje- og egenpresentasjonsmateriell, osv. – inngår også i datagrunnlaget. I tillegg ble representanter for andre institusjoner og organisasjoner intervjuet: Fornyings- og Administrasjonsdepartementet, Kommunenes Sentralforbund, Nasjonal Sikkerhetsmyndighet, Norsk Senter for Informasjonssikring, Personvernnemnda, Foreningen for Kommunal Informasjonssikring og representanter for konsulentbransjen. Til sammen ble 62 intervjuer gjennomført.

tene formidler et overdrevent inntrykk av kommunenes evne til å iverksette et informasjonssikkerhetsarbeid basert på prinsippet om risikostyring.

Organisatoriske utfordringer

Offentlig sektor generelt og kommunene spesielt, er viktige brukere av sikkerhetsbestemmelsene i personopplysningsloven og forskriften:

> *De offentlige virksomhetene i Norge sitter samlet sett på nærmest ufattelige mengder informasjon om innbyggerne (…) Individet har i liten grad mulighet til å påvirke hvilke former for opplysninger som samles inn og lagres.*[9]

På kommunenivå er det særlig innenfor helse, pleie/omsorg og skole at store mengder personopplysninger behandles. Hvordan disse opplysningene sikres mot brudd på konfidensialiteten, integriteten og tilgjengeligheten har derfor potensielt stor betydning for den enkeltes personvern og for innbyggernes tillit til det administrative og tjenesteproduserende apparatet. Spørsmålet er derfor hvordan de rettslige kravene til organisering og gjennomføring av informasjonssikkerhetsarbeidet ivaretas i den kommunale delen av offentlig sektor?

Alle de 19 kommunene i studien hadde gjennomført organisatoriske endringer som var i tråd med bestemmelsene i personopplysningsloven og forskriften. For eksempel var det stadfestet at rådmannen (den daglige ledelsen) var den øverste ansvarlige for sikkerhetsarbeidet, og det operative (eller daglige) ansvaret for arbeidet var delegert til en sikkerhetsleder. En sikkerhetsorganisasjon var derfor (i teorien) etablert. Men det var også visse variasjoner i hvordan bestemmelsene ble etterlevd: noen kommuner hadde nedlagt et større arbeid og lykkes bedre med å følge reglene enn andre. Til tross for at sikkerhetsorganisasjoner var etablert, og selv om det varierte noe hvor godt kommunene hadde lykkes med å etterleve de øvrige bestemmelsene, var det generelle bildet at det var relativt store avvik mellom bestemmelsenes bokstav og kommunenes regelpraksis. Fem av kommunene hadde riktignok fått på plass store deler av det lovpålagte organisatoriske rammeverket, men i de resterende 14 kommunene var situasjonen en annen.

I disse kommunene kan holdningene til regelverket og praktiseringen av kravene til organisering og gjennomføring oppsummeres på denne måten:

---

9 Brev fra Datatilsynet til Fornyings- og administrasjonsdepartementet, 31. august 2007, s. 1. Det betyr at kommunene står høyt på Datatilsynets liste over prioriterte tilsynsobjekter. Den største tilsynsrunden i kommunesektoren ble gjennomført i 2003. Da ble 35 kommuner kontrollert (se *Datatilsynets årsmelding 2003*).

- De regulatoriske målsettingene (informasjonssikkerhet og personvern) oppfattes som viktige og riktige – kommunene ønsker å følge regelverket.
- Regelverket oppleves som problematisk å forstå – det inneholder mange begreper som det kan være vanskelig å se den praktiske relevansen av.
- Rådmennene har det formelle styringsansvaret, men har liten interesse av å styre sikkerhetsarbeidet.
- Sikkerhetslederne har det operative/daglige ansvaret for sikkerheten, men er skeptiske til for sterk rådmannsstyring.
- Sikkerhetslederne har problemer med å nå ut til kommunens ansatte med informasjon om rettslige plikter og interne sikkerhetsrutiner.
- Sikkerhetslederne (og de IT-ansatte) har jobbet med informasjonssikkerhet på en prosjektbasert (eller ad hoc-preget) måte, men dagens regelverk krever langt større grad av byråkratisk systematikk og planmessighet.
- Regelverket oppleves som dårlig tilpasset informasjonssikkerhetsproblemets omfang – det «skyter spurv med kanoner».

Dette viser at kommunene hadde (eller uttrykte) et genuint ønske om å gjøre som regelverket krever, men at i det store flertallet av kommunene støtte etterlevelsesarbeidet mot viktige hindringer: interne organisatoriske barrierer (vanskelig å involvere rådmannsnivået og de ansatte i sikkerhetsarbeidet) og utfordringer knyttet til innføringen av nye arbeids- og styringsformer (fra prosjektorganisering til mer byråkratisk planmessighet og skepsis mot sterkere rådmannsstyring). I tillegg kom problemer av mer rettslig karakter (reglene oppfattes som for omfattende og vanskelige å forstå). Ønsket om å følge regelverket kan derfor sies å være større enn evnen til faktisk å gjøre det.

På et område var imidlertid avstanden mellom hva regelverket krever og hva kommunene gjorde mindre enn i forhold til kravene til organisering og gjennomføring av sikkerhetsarbeidet: bestemmelsene om utarbeidelse av styrende dokumentasjon.

Styrende dokumenter

Ovenfor så vi at personopplysningsloven og forskriften legger vekt på at det utarbeides såkalte styrende dokumenter. Vi så også at disse dokumentene omfatter beskrivelser av kommunenes sikkerhetsorganisasjon (fordelingen av ansvar og oppgaver), sikkerhetsmål, sikkerhetsstrategi, opplegg for gjennomføring av risikovurderinger og sikkerhetsrevisjoner, rutiner for sikker behandling av personopplysninger og rutiner for ledelsens gjennomgang av styringssystemet for informasjonssikkerhet. En viktig del av etterlevelsesarbeidet består derfor i å lage og oppdatere lokale planverk.

Til tross for at det var visse avvik mellom regelverkets dokumentasjonskrav og det planverket som kommunene hadde utarbeidet, hadde 17 av de 19 kommunene laget mesteparten av de styrende dokumentene som personopplysningsloven og forskriften krever (i den ene av de to kommunene som ikke hadde planverket på plass, foregikk utarbeidelsen av tilsvarende dokumentasjon).[10] Likevel mente et stort flertall av de intervjuede at det var dårlig sammenheng mellom det dokumentene beskrev og kommunenes reelle regelpraksis.[11] Flere av dem hadde derfor et relativt kynisk forhold til dokumentasjonskravene i loven og forskriften. Enkelte hevdet for eksempel at mange kommuner – deres egen inkludert – hadde søkt på Internettet for å finne eksempler på hvordan bl.a. en sikkerhetsorganisasjon, sikkerhetsmål, sikkerhetsstrategier, opplegg for risikovurderinger og rutiner for kommuneledelsens gjennomgang av sikkerhetsarbeidet kunne beskrives. Så hadde de klipt og limt fra disse dokumentene – eller kopiert alle dokumentene og satt inn navnet på sin egen kommune i overskriften. Konsekvensen av dette var, ifølge de som hevdet dette synspunktet, at de styrende dokumentene hadde begrenset operativ verdi: sikkerhetsorganisasjonen eksisterte bare på papiret, sikkerhetsmål og strategier var i beskjeden grad styrende for arbeidet, opplegg for risikovurderinger ble ikke gjennomført og rutiner for ledelsesgjennomganger ble ikke praktisert.[12]

Spesielt bruken av rutiner for risikovurdering fremstod som problematisk. Utgangspunktet i personopplysningsloven og forskriften er at risikovurderinger skal gi svar på spørsmålet «hva trenger vi å forbedre for at informasjonssikkerheten i vår kommune skal være tilfredsstillende?» Alle kommunene som deltok i undersøkelsen hadde laget rutiner for hvordan dette spørsmålet skulle besvares. Men ansvaret for å finne svaret, det vil si å gjennomføre risikovurde-

10 Det ble ikke gitt tilgang til oversikter over hvordan kommunenes informasjonssystemer var oppbygd (såkalte konfigurasjonskart). Disse oversiktene hører til blant de styrende dokumentene, men gis ikke ut av sikkerhetsgrunner.

11 I kommuner hvor sikkerhetslederne eller IKT-sjefene ikke uttrykte slike oppfatninger, var årsaken vanligvis at arbeidet med regeletterlevelse var såpass nytt at man vanskelig kunne vurdere hvordan forholdet mellom ord og handling ville utvikle seg.

12 Avviksmeldingssystemer er en annen del av kommunenes informasjonssikringsarbeid hvor teori og praksis var to litt ulike ting. Systemer for avviksmelding er vanligvis en del av kommunenes intranett, og meningen er at sikkerhetsmessige feil eller mangler skal rapporteres på egne elektroniske skjemaer. Skjemaene sendes enten til virksomhetslederen og/eller til kommunens sikkerhetsleder for videre behandling (men hvis det er snakk om alvorlige avvik, skal beskjed formidles helt opp til rådmannen). Flere av kommunene i denne studien hadde brukt store pengesummer på å skaffe seg et avviksmeldingssystem, men systemene ble lite brukt (en kommune rapporterte at den i løpet av de siste to årene hadde fått inn fire meldinger om sikkerhetsproblemer gjennom avviksmeldingssystemet). Isteden ble informasjon om feil eller mangler formidlet via andre kanaler – gule lapper, e-post, telefon – eller ikke i det hele tatt.

ringer, var delegert til de ulike kommunale virksomhetene (skoler, barnehager, sykehjem, sosialkontorer, osv.). Resultatet av denne praksisen fremstod som todelt. For det første at i den grad risikovurderinger ble gjennomført, skjedde dette med lange og uregelmessige mellomrom, mens regelverket krever at vurderingene gjennomføres relativt hyppig og rutinemessig.[13] For det andre at sikkerhetslederne hadde liten oversikt over hvorvidt de kommunale virksomhetenes fulgte opp rutinene eller ikke. Det generelle inntrykket var derfor at de rutinene som dokumentene beskrev enten ikke var forankret hos de som skulle utføre arbeidet eller at sikkerhetslederne manglet kunnskap om graden av forankring og oppfølging.[14]

Flertallet av sikkerhetslederne ga også uttrykk for at opparbeidelsen av styrende dokumenter, bl.a. retningslinjer for gjennomføring av risikovurderinger, var et resultat av prosjektbasert innsats. Det var et skippertak som kommunene hadde gjort i løpet av en relativt kort periode (vanligvis to-tre måneder), men å sørge for at arbeidsmessige endringer fulgte i kjølvannet av det skrevne ord – ble tilpasset beskrivelsene i dokumentene – var et spørsmål som ikke hadde fått like stor oppmerksomhet. Den organisatoriske planmessigheten og systematikken som dokumentene beskrev var derfor noe man hadde som mål å nærme seg, men det daglige sikkerhetsarbeidet var fortsatt ad hoc-preget, og handlet i stor grad om å løse tekniske eller andre problemer etterhvert som de oppstod.

Som antydet ovenfor, hadde fem av kommunene lagt ned en spesielt stor egeninnsats for å få på plass den lovpålagte dokumentasjonen. Dette var også de kommunene som hadde gjort mest for å tilpasse det operative sikkerhetsarbeidet til regelverkets krav og dokumentenes innhold. Dermed kan det hevdes at det var en viss positiv sammenheng mellom arbeidet med å ivareta dokumentasjonskravene og arbeidet med å overholde de øvrige bestemmelsene i regelverket. Det generelle bildet var imidlertid at det var påfallende store for-

13 I enkelte kommuner deltok sikkerhetslederen som instruktør eller konsulent i den første runden med risikovurderingen som kommunen hadde gjennomført. Deretter var det meningen at virksomhetene selv skulle initiere og gjennomføre risikovurderinger. I de fleste tilfellene førte dette til at den første risikovurderingen også ble den (foreløpig) siste. Samtidig ble risikovurderinger i første rekke benyttet ved anskaffelse og installering av nye IT-systemer, men regelverket krever at slike vurderinger skal brukes ved alle endringer (for eksempel organisatoriske eller bygningstekniske) som kan ha betydning for informasjonssikkerheten (se personopplysningsforskriften § 2-4). Flere av sikkerhetslederne antydet at de i fremtiden måtte bli mer aktive pådrivere for å få iverksatt og gjennomført risikovurderinger.

14 Dette inntrykket bekreftes i intervjuer med ansatte i Datatilsynet og understøttes av kontrollfunn fra kommunesektoren. Et gjennomgående trekk i kontrollrapportene, er at kommunene ikke hadde brukt risikovurderinger som grunnlag for beslutninger om iverksettelse av sikkerhetstiltak.

skjeller mellom dokumentbeskrivelsene og intervjuobjektenes egne fremstillinger av hvordan planverket ble praktisert. Det var også påfallende at innholdet i dokumentasjonen var relativt lik på tvers av kommuner. I tillegg til at enkelte kommuner hadde hentet inspirasjon fra andre kommuner, kan dokumentlikheten henge sammen med at informasjonssikkerhet er et område hvor konsulentbransjen har gjort seg sterkt gjeldende. 1/3 av kommunene i undersøkelsen hadde derfor fått assistanse fra konsulentfirmaer som tilbød standardløsninger for hvordan dokumentasjonskravene i personopplysningsloven og forskriften kunne imøtekommes. Dessuten finnes en rekke ikke-kommersielle aktører som tilbyr maler for eller eksempler på hvordan planverket kan utformes.[15] Dette kan ha bidratt til at deler av sikkerhetsdokumentasjonen hadde et lite lokalt, men et noe standardisert og «masseprodusert» preg.

Den manglende sammenhengen mellom dokumentinnhold og kommunal regelpraksis innebar bl.a. at hvor godt sikkerhetsorganisasjonen fungerte – spesielt graden av forankring på rådmannsnivået – hadde mindre å gjøre med den formelle ansvars- og oppgavefordelingen, men avhang i stor grad av personlige relasjoner.[16] Særlig to forhold syntes å ha betydning her. For det første «kjemien» mellom rådmannen og sikkerhetslederen – kjente de hverandre og hvor godt snakket de sammen? For det andre hvorvidt sikkerhetslederen var en god organisasjonspolitiker (eller ikke): hvor dyktig var han eller hun til å sette regeletterlevelse på kommuneledelsens dagsorden og til å få gjennomslag for sine argumenter? I tillegg til personlige relasjoner, syntes institusjonelle forhold å ha en viss betydning, spesielt om kommunene hadde opprettet en ordning med personvernombud eller ikke.[17] I de to kommunene som hadde etablert en personvernombudsordning, virket det som om sikkerhetslederen hadde lettere for å få gjennomslag for sine synspunkter enn i kommuner hvor en slik ordning ikke eksisterte.[18] Det skyldes trolig at sikkerhetslederen kunne støtte seg på personvernombudet i arbeidet med å få kommuneledelsen til å

15 For eksempel Foreningen for Kommunal Informasjonssikkerhet (www.kins.no) og Norsk Senter for Informasjonssikring (www.norsis.no).

16 Dette er ikke overraskende. At det er forskjell mellom formelle og reelle strukturer er gamle nyheter for organisasjonsforskere. For diskusjon, se for eksempel Scott og Davis 2007.

17 Personvernombud er en ordning hvor kommuner (og andre virksomheter i privat eller offentlig sektor) utpeker en person som skal ha et spesielt ansvar for å påse at reglene om behandling av personopplysninger ivaretas (for en nærmere beskrivelse av ordningen, se www.datatilsynet.no).

18 Det syntes også å ha en viss betydning om rådmannen var opptatt av kvalitetsstyring. Der hvor kommuneledelsen var opptatt av dette, økte sannsynligheten for at reglene om informasjonssikring fikk en viss oppmerksomhet. Det skyldes trolig at kvalitetsstyring og informasjonssikring baserer seg på den samme tenkemåten: metodikken og styringsprinsippene er de samme.

prioritere etterlevelsen av regelverket, mens denne støtten manglet i kommuner hvor ordningen ikke fantes. [19]

Etterlevelsesillusjonen

Den effekten av dokumentasjonskravene som er drøftet ovenfor – det gis et inntrykk av relativ bokstavnær regeletterlevelse som ikke stemmer med faktisk regelpraksis – var i begrenset grad en bevisst strategi: dokumentene ble ikke skrevet med tanke på å skape en bestemt virkning hos et bestemt publikum (for eksempel at Datatilsynet skal få et fordelaktig syn på kommunenes evne og vilje til å overholde bestemmelsene om informasjonssikkerhet). Hovedforklaringen må isteden søkes andre steder:

Vi har sett at praktiseringen av regelverket ble påvirket av en rekke organisatoriske hindringer (manglende ledelsesforankring, liten involvering av de ansatte, uvante arbeids- og styringsformer, osv.), men vi har også sett at disse hindringene i mindre grad hadde betydning for utformingen av sikkerhetsdokumentasjonen. Dermed oppstod et misforhold mellom dokumentinnhold og praktiseringen av de øvrige sikkerhetsbestemmelsene som førte til at beskrivelsene av regelpraksis ikke stemte med faktisk regelpraksis. Det er dette misforholdet – det kommunene skriver harmonerer ikke helt med hva de gjør – som kan beskrives som en etterlevelsesillusjonen.

Etterlevelsesillusjonen – hva den er og hvilke konsekvenser den kan ha – kan tydeliggjøres med følgende eksempel:

> *The traffic light changes when a pedestrian is halfway across the intersection. As long as the pedestrian is not in imminent danger from the oncoming traffic, a small dramatization is likely to ensue. He lifts his knees a bit higher for a step or two, simulating haste, thereby implicitly recognizing the motorist's right-of-way. In fact, in nearly all cases, if my impression is correct, the actual progress of the pedestrian across the intersection is no faster than it would have been if he had simply proceeded at his original pace. What is conveyed is the impression of compliance without its substance. But the symbolic order, the right of the motorist to the road, is not directly challenged; indeed, it is confirmed by the appearance of haste. It is*

19 Samtidig indikerer opprettelsen av personvernombud at kommunene var spesielt opptatt av å overholde regelverket. Det kan derfor tenkes at det var opptattheten av regeletterlevelse (snarere enn selve ombudsordningen) som gjorde at sikkerhetsledernes gjennomslagskraft økte.

almost as if symbolic compliance is maximized precisely in order to minimize compliance at the level of actual behaviour [min utheving].[20]

Med utgangspunkt i dette eksemplet, kan enkelte karakteristiske trekk ved etterlevelsesillusjonen fremheves:

- Det skapes et inntrykk av at regelverket overholdes (fotgjengeren simulerer hastverk når trafikklyset skifter fra grønt til rødt).
- Inntrykket gjør det mulig å handle på måter som ikke harmonerer med regelverkets bokstav (fotgjengeren går på rødt lys).
- Inntrykket skapes fordi det ikke er ønskelig å utfordre den rettslige orden (fotgjengerens simulerte hastverk signaliserer respekt for trafikkreglene).
- Inntrykket skapes av den parten som ikke har retten på sin side (fotgjengeren).
- Inntrykket formidles til (og aksepteres av) den parten som har retten på sin side (bilisten).

Etterlevelsesillusjonen innebærer at overholdelsen av rettslige reguleringer består av to nivåer: et offentlig ansikt (inntrykket av etterlevelse som formidles til omgivelsene) og et praksisnivå (handlinger eller tiltak som ikke harmonerer med regelverkets intensjon eller bokstav). Det er på det første nivået – etterlevelsens offentlige ansikt – at inntrykket av regeloverholdelse (eller, i det minste, respekt for regelverket) oppstår, men det er på praksisnivået at dette har konkrete effekter. Den viktigste effekten er at så lenge man gir inntrykk av å overholde reglene, og så lenge omgivelsene har en positiv oppfatning av viljen til å følge lover og forskrifter, trenger man ikke å handle slik som regelverket strengt tatt krever (for eksempel at fotgjengeren stopper og venter på grønt lys før han krysser veien). Dermed kan aktørene få både i pose og sekk: inntrykket av etterlevelse anerkjennes av omgivelsene som respekt for regelverket og mangelen på faktisk etterlevelse gjør at aktørene slipper å betale de reelle etterlevelseskostnadene.

Etterlevelsesillusjonen og kommunene

Men selv om pliktsubjektene (kommunene) kan nyte visse fordeler av etterlevelsesillusjonen, betyr ikke dette at fordelene som høstes er planlagt og villet. I kommunene som har deltatt i denne studien synes det derfor ikke riktig å si at misforholdet mellom dokumentinnhold og regelpraksis skyldes opportunisme,

20 Scott 1985: 26. Tilsvarende måter å forstå regeletterlevelse på diskuteres bl.a. i March et al. 2000: 14-16, Heimer 1996, Edelman 1992 eller Sitkin og Bies 1994.

men sviktende evne til å gjøre som regelverket sier. Spesielt viktig synes det å være at kommunene hadde begrensede ressurser å sette inn i arbeidet med å løse de mange og tunge utfordringene som kravene til organisering og gjennomføring reiste.

Utgangspunktet her er at selv om alle kommunene hadde utpekt en sikkerhetsleder, utgjorde ikke rollen som leder for sikkerhetsarbeidet en full stilling. I de største kommunene som var med i undersøkelsen, var det vanligste at stillingsprosenten lå på omkring 50 (eller noe høyere). I flertallet av kommunene lå den imidlertid på 30 prosent eller mindre. Det betyr at til tross for at sikkerhetslederne fremstod som engasjerte ildsjeler, stod den kommunale ressursbruken neppe i forhold til hva som kreves for å etterleve regelverket fullt ut. Derfor er det heller ikke så overraskende at det oppstår en etterlevelsesillusjon. For når de kommunale ressursene er relativt få og små, er det ikke urimelig at etterlevelsen konsentreres om de reglene som (a) er relativt lite kostnadskrevende å overholde, (b) lett kan vises frem for omgivelsene (Datatilsynet og andre eksterne aktører) og/eller (c) krever liten grad av organisatorisk endring. Overholdelse av dokumentasjonskravene prioriteres derfor fordi det er mindre problematisk og ressurskrevende å skrive at regelverket etterleves enn å gjennomføre det man skriver.

Det inntrykket som dermed skapes kan likevel være verdifullt. Poenget er at etterlevelse av dokumentasjonskravene gir et synlig bevis på at kommunene har gjort en innsats for å følge opp bestemmelsene i loven og forskriften. Intern praksis – om kommunene faktisk endrer organiseringen og gjennomføringen av sikkerhetsarbeidet i tråd med det som står i dokumentene – synliggjør ikke regeletterlevelse på samme måte som det dokumentbeskrivelser gjør. Hva man foretar seg i det daglige kan ikke alltid settes i permer, legges ut på intranettet, presenteres på kommunenes hjemmesider eller sendes til Datatilsynet. Dokumentasjonen synes derfor å spille en dobbeltrolle i etterlevelsesarbeidet: den viser kommunenes «gode hensikter» samtidig som den «dekker over» mangelfull intern praksis. Dokumentene demonstrerer at selv om viktige deler av regelverket ikke etterleves slik som forutsatt, har kommunene vilje til å opptre som lojale og samvittighetsfulle regelbrukere.[21]

21 I reguleringslitteraturen finnes liknende analyser av betydningen av formell dokumentasjon. Her hevdes det for eksempel at: «(…) organizational members devote at least part of their labour to the creation of a desired impression as expressed by means of documentation. Records thus have a rhetorical use as, for instance, when they are used to convince some audience that those in the organization are taking care of business in quite proper ways» (Maanen og Pentland 1994: 53). Se også Brunsson et al. 2000 eller Power 1997.

Datatilsynet

Spørsmålet er om eksternt press, fra Datatilsynet eller andre aktører, kan bidra til å redusere (men trolig ikke eliminere) etterlevelsesillusjonen? Denne muligheten er til stede. Oppslag i lokalmedia om sikkerhetsbrudd har for eksempel vært en katalysator for endringer i praktiseringen av regelverket i enkelte av de kommunene som har deltatt i denne studien. I tillegg krever regelverket at kommuner (og andre virksomheter) ikke bare dokumenterer det interne ledelsessystemet for informasjonssikkerhet, men at det også føres fortegnelser over de aktiviteter som systemet skal ivareta (for eksempel iverksatte sikringstiltak, resultater av risikovurderinger, behandlingen av sikkerhetsbrudd eller ledelsens gjennomgang av sikkerhetsmål og strategier). Denne aktivitetsbaserte dokumentasjonen vil kunne indikere om ledelsessystemet faktisk fungerer eller om det er mest til pynt.

Utfordringen er at det ikke er andre enn Datatilsynet som kan kreve innsyn i disse dokumentene.[22] Det betyr at selv om den aktivitetsbaserte dokumentasjonen kan vise om ledelsessystemet brukes til å utføre lovpålagte oppgaver eller ikke, vil den praktiske betydningen av denne kontrollmuligheten avhenge av omfanget av Datatilsynets tilsynsressurser. Men til tross for at kommunesektoren er mer i Datatilsynets søkelys enn de fleste andre bransjer og sektorer, har det likevel begrensede muligheter til å sjekke sammenhengen mellom liv og lære i kommunenes sikkerhetsarbeid.[23] Årsaken er at Datatilsynet er blant landets minste tilsynsorganer.[24] Samtidig som det har et svært omfattende tilsynsansvar: det skal informere om regelverket og kontrollere regeletterlevelsen i alle bransjer og sektorer hvor personopplysninger behandles. Følgelig virker det lite realistisk å tro at Datatilsynet alene kan løse alle utfordringer knyttet til praktiseringen av informasjonssikkerhetsbestemmelsene som etterlevelsesillusjonen reiser.

---

22 Kommunens innbyggere kan få innsyn i sikkerhetsdokumentasjonen så lenge innsyn ikke svekker informasjonssikkerheten (se personopplysningsloven § 18). Dermed vil de fleste aktivitetsbaserte dokumentene være unntatt offentlighet.

23 I tillegg til at det foreligger en etterlevelsesillusjon på personvernområdet, kan det også sies å eksistere en håndhevelsesillusjon. Håndhevelsesillusjonen går ut på at kommuner som i liten grad hadde vært i kontakt med Datatilsynet, syntes å tro at Datatilsynet var en stort byråkrati som rådde over kraftige og hyppig brukte sanksjonsvirkemidler. Men etter at personopplysningsloven og forskriften trådte i kraft, har ikke Datatilsynet brukt sterkere lut enn pålegg om lukking av avvik i kommunesektoren (for ulike syn på effekten av forskjellige sanksjonsformer, se for eksempel Hawkins 2002, Kagan og Scholz 1984 eller Bardach og Kagan 1982). Det er likevel vanskelig å vite om håndhevelsesillusjonen har bidratt til å styrke kommunenes bestrebelser på regeletterleve.

24 I 2008 forvaltet Datatilsynet 35 årsverk og et budsjett på litt i overkant av 26 millioner kroner.

Avslutning

De empiriske funnene som er drøftet i denne artikkelen viser at det i de studerte kommunene var viktige utfordringer knyttet til rettslig regulering av informasjonssikkerhet på personvernområdet. Utfordringene kan oppsummeres på følgende måte:

- Overholdelsen av enkelte deler av regelverket er mer problematisk enn overholdelse av andre deler.
- De delene av regelverket som er problematisk å overholde, dreier seg om implementering av nye organisatoriske strukturer, rutiner og arbeidsformer.
- De delene av regelverket som er enklere å overholde, dreier seg om utforming av ulike typer dokumenter og planverk.
- Misforholdet mellom de delene av regelverket som er enkle og de delene som er vanskelige å overholde, gjør at det oppstår en etterlevelsesillusjon: det kommunene sier de gjør stemmer bedre med regelverket enn det de faktisk gjør.
- Etterlevelsesillusjonen innebærer ikke fravær av organisatorisk endring, men endringene fremstår som mer i tråd med regelverket enn hva de i virkeligheten er.
- Etterlevelsesillusjonen skapes ikke for å «lure» staten (Datatilsynet) eller andre eksterne aktører, men skyldes at regeletterlevelsen støter mot organisatoriske hindringer og ressursmessige beskrankninger.

Hovedkonklusjonen er derfor at kommunene ikke implementerer rettsregler på en mekanisk og forutsigbar måte. I kommunal sektor og på informasjonssikkerhetsområdet kommer dette til uttrykk ved at (a) arbeidet med regeletterlevelse har uintenderte effekter (det oppstår et ikke-planlagt og overdrevent inntrykk av kommunal regeltroskap) og (b) dette skyldes at ønsket om å gjøre som regelverket krever møter interne barrierer (organisatoriske og ressursmessige) som hindrer at ønsket oppfylles.

Litteratur

Bardach, Eugene og Robert A. Kagan (1982): Going by the Book. The Problem of Regulatory Unreasonableness. Philadelphia: Temple University Press.

Brunsson, Nils et al. (2000): A World of Standards. Oxford: Oxford University Press.

Collingridge, David (1980): The Social Control of Technology. London: Frances Pinter.

Daler, Torgeir et al. (2002): Håndbok i datasikkerhet. Informasjonsteknologi og risikostyring. Trondheim: Tapir akademiske forlag.

Edelman, Lauren B. (1992): *Legal Ambiguity and Symbolic Structure: Organizational Mediation of Civil Rights Law*. American Journal of Sociology, 97, s. 1531-1576.

Hawkins, Keith (2002): Law as the Last Resort. Prosecution Decision-Making in a Regulatory Agency. Oxford: Oxford University Press.

Heimer, Carol A. (1996): *Explaining Variation in the Impact of Law: Organizations, Institutions, and Professions*. Studies in Law, Politics and Society, vol. 15, s. 29-59.

Johansen, Michal Wiik et al. (2001): Personopplysningsloven. Kommentarutgave. Oslo: Universitetsforlaget.

Kagan, Robert A. og John T. Scholz (1984): *The Criminology of the Corporation and Regulatory Enforcement Strategies*. I Keith Hawkins og John M. Thomas (red.): Enforcing Regulation. Law in a Social Context. Boston: Kluwer-Nijhoff.

Maanen, John Van og Brian T. Pentland (1994): *Cops and Auditors: The Rhetoric of Records*. I Sim B. Sitkin og Robert J. Bies (red.): The Legalistic Organization. Thousand Oaks: Sage Publications.

March, James G. et al. (2000): The Dynamics of Rules. Change in Written Organizational Codes. Stanford: Stanford University Press.

Saltmarsh, Timothy J. og Peter S. Browne (1983): *Data Processing – Risk Assessment*. I Marvin M. Wofsey (red.): Advances in Computer Security Management. Chichester: John Wiley.

Power, Michael (1997): The Audit Society. Rituals of Verification. Oxford: Oxford University Press.

Schartum, Dag Wiese (2005): *Krav til sikring av personopplysninger*. I Arild Jansen og Dag Wiese Schartum (red.): Informasjonssikkerhet. Rettslige krav til sikker bruk av IKT. Bergen: Fagbokforlaget.

Schneier, Bruce (2000): Secrets and Lies. Digital Security in a Networked World. New York: John Wiley.

Scott, Richard W. og Gerald F. Davis (2007): Organizations and Organizing. Rational, Natural, and Open System Perspectives. Upper Saddle River: Pearson Education.

Seipel, Peter (red.) (2006): Rätten och säkerheten i IT-samhället. Stockholm: Jure AB.

Sitkin, Sim B. og Robert J. Bies (1994): *The Legalization of Organizations. A Multi-Theoretical Perspective*. I Sim B. Sitkin og Robert J. Bies (red.): The Legalistic Organization. Thousand Oaks: Sage Publications.

Slay, Jill og Andy Koronios (2006): Information Technology Security and Risk Management. Sydney: John Wiley.

Andre kilder

Brev fra Datatilsynet til FAD, 31. August 2007.

Datatilsynets årsmelding 2003.

Personopplysningsloven – Lov om behandling av personopplysninger (personopplysningsloven) av 14.april 2000 nr 31.

Personopplysningsforskriften - Forskrift om behandling av personopplysninger (personopplysningsforskriften) av 15.desember 2000 nr 1265.

NABOLANDS-TV. EN INNFØRING I LANDSKAPET[1]

Helge M. Sønneland

Det er prisverdig at Nordisk ministerråd igjen tar opp spørsmålene som «nabolandsfjernsyn» reiser, og holder fast ved målsettingen å gjøre nabolandenes fjernsynsprogrammer tilgjengelig i størst mulig utstrekning. Problemstillingene dette reiser i vår digitale tid, er langt på vei de samme som under «Nordsat-prosjektet» for 25 år siden. Jeg skal i dette innlegget si litt om dette landskapet, og også gi et visst historisk tilbakeblikk. Den aktuelle situasjon beskrives i advokat Ann Grew Pfeiffers kapitel.

Jeg avgrenser min gjennomgang her til å gjelde program fra det som på norsk heter allmennkringkasterne – dvs (i det minste hovedsendingene) til de kringkastingsselskapene som har et «public service»-oppdrag – og vi snakker om *samtidig, uendret videresending* – for dersom det skjer opptak eller endringer innen videresendingen skjer, blir problemene andre og enn mer komplekse.

Min fremstilling her avgrenser jeg i det vesentlige også mot formidling av nabolands – program til og i landene i Vest-Norden – som reiser spesielle spørsmål. Jeg vil si litt om hva som har vært, og til dels er, problemene, og om hvordan de er søkt løst.

Litt historikk

Siden første gang det fra politisk hold ble uttrykt ønske om å gjøre nabolands-tv tilgjengelig, har økt tilgang og økt spredning vært målet. At vi i mellomtiden har fått et vell av andre, kommersielle tilbud, har vel snarere gjort behovet større enn mindre.

På 1970-tallet tok elektriker-firmaer, og de som solgte tv-apparater, initiativ til å ta imot og spre videre tv-signaler som de fanget opp fra naboland – først og fremst for å legge ut kabel, som igjen genererte salg av tv-apparater. Dette var attraktivt for publikum i en tid hvor de nasjonale tilbud var begrenset til en eller to kanaler fra de nasjonale selskapene.

Dermed ble grunnlaget lagt for det som siden skulle bli informasjons-motorveger – etter hvert koplet opp til og erstattet av fiberoptikk. Svenske program ble spredt i Østlandsområdet i Norge, i Øresundsområdet så man de

1 Publisert i Nordicom Information 3-2009 : Nabolands TV i en digital tidsålder, s. 11-19.

respektive nabolandsprogrammene, i Syd-Danmark tyske program, og Sverige og Finland inngikk bilateral avtale om gjensidig spredning av deler av programflaten, til glede for finsk-talende i Sverige og svensk-talende i Finland.

Etter anmodning fra Nordisk råd, tok Nordisk ministerråd tidlig på 1970-tallet initiativ til å utrede muligheten for å spre nabolandenes tv via bakkenett – altså parallelt med eget lands sendinger[2].

Det ble etter hvert gjennomført flere utredninger, og det ble klart at videredistribusjon i bakkenett ville bli svært kostbart rent teknisk – i tillegg til program – og oversettelseskostnader, og at det var kapasitetsproblemer mht frekvenser.

Men: gjennom høringsrunden av disse første rapportene ble man klar over mulighetene som kunne ligge i den nye teknologisk utvikling: satellittene var på vei inn på vår mediepolitiske arena. Den gang ble det skilt mellom i to hovedkategorier; *kommunikasjons-satellitter* – som sendte fra et punkt til et eller flere andre dedikerte punkt (som oftest beregnet for videresending); og *direktesendende* satellitter. De var den gang under planlegging, og signalene skulle kunne tas imot av relativt små parabolantenner direkte av husholdningene. Dermed endret man siktemål, og etablerte etter en første forundersøkelse en statssekretærgruppe som vurderte mulighetene for å anvende satellitter. Gruppen kom med en positiv tilråding[3]. Den ble fulgt opp i den såkalte Nordsat-studien, et omfattende og dyptpløyende arbeid, både mht programspørsmål, juridiske spørsmål og teknologi – og selvsagt økonomi[4].

Jeg skal ikke si meget om Nordsat-prosjektet: litt spissformulert og i ettertid vil jeg karakterisere det som et program – samarbeidsprosjekt som i første runde søkte en satellitt som bare fantes på tegnebrettene – nemlig en direktesendende satellitt som kunne romme alle de aktuelle 7-8 kanalene, og som egentlig var for tung til å skytes opp med datidens raketter. I neste runde – fra 1982 – gikk det over til å bli et prosjekt hvor en for liten, men direktesendende, satellitt, nemlig den svenske Tele-X med sine 3 kanaler – søkte et nordisk programsamarbeid tilpasset satellitten[5]. Det endelige sammenbruddet ble møtt med glede av mange kulturarbeidere som syntes det ville bli for mye tv: «*skit er skit – om än per satellit*» som det het på en plakat.

Gjennom mange ministerrådsmøter, hvor middagenes kvalitet var omvendt proporsjonal med innholdet i beslutningene – strandet m.a.o prosjektet til slutt. Riktignok ikke uten at også en løsning med sendinger på ***én*** (kommunikasjonssatellitt-) kanal, som skulle bringe programmer fra alle de nordiske

2 NU 1972: 7, fulgt opp i april 1974 (Naboland-TV – utredning av Nordisk teknisk TV-utvalg), og i sluttrapporten «TV över grenserna», NU 1974:19.
3 Nordisk radio och television via satellit, NU serien A 1977:7
4 Nordisk radio och television via satellitt NU serien A 1979:4
5 Nordisk radio-och TV-samt telesamarbete via satellit. NU 1984:8

kringkasterne, var utredet. Den utredningen ble sørgelig nok forlatt, også av kringkasternes selv – bl.a. av mangel på tiltro både til interessen for egne programmer (bare 2 % av befolkningen ville se kanalen, og det mente man var for lite), og mangel på tiltro til at sendeskjemaene ville holde tidsmessig – hva skulle man vel gjøre om nyhetene i Yle ble litt for langtrukne før man satte over til de danske?

Muligheten for å lage én, felles kanal ble vurdert nok en gang et ti-år senere, men ble også da lagt til side, ikke minst av økonomiske grunner. Spesielt tyngende ville oversettelseskostnadene være. Og siden alt tydet på at kringkastingsselskapene ville bli belastet kostnadene, var det ikke urimelig at deres begeistring var begrenset.

Men underveis mot Nordsat-prosjektets endelikt, drøftet en del av oss nordiske og departementale tjenestemenn om det ikke ville være mulig å legge til rette for økt spredning av nabolands-tv i de land der den rent faktisk allerede fantes – og for å undersøke de rettslige problemene som reiste seg. Nordisk ministerråd sa seg enig, og etablerte en nordisk embetsmannsgruppe. Den fikk som mandat å utrede de rettslige spørsmål knyttet til spredning av nabolands-tv, først og fremst i kabel.

Dette arbeidet, som det er få tilsvarende eksempler på i nordisk sammenheng, resulterte i utredningen «Nabolands-tv i kabel». Den ble fremlagt i mars 1984[6]. De forslag som der ble fremlagt resulterte i en felles nordisk forståelse, og ble ført videre av de nordiske lands ansvarlige departementer. Resultatet ble en nasjonal lovgivning i de nordiske land som i stor grad er harmonisert, og som i hovedsak gjelder den dag i dag[7].

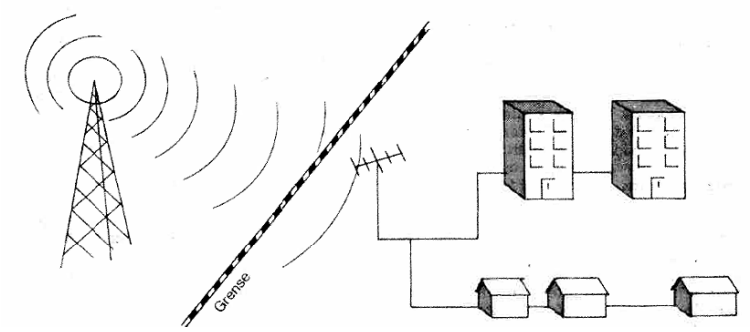
Ca 10 år senere – i 1992 til 1994 – gjorde ministerrådet opp status, og konstaterte at det var begrenset rom for nordiske politiske initiativ for å få øket nabolands- spredningen[8]. Men positivt nok kunne videresending av dansk TV i realiseres i norske kabelnett etter sterk påvirkning av de to lands statsministre.

Nordisk råd – som gjennom snart 40 år har tatt en rekke initativ, og som har bidratt til å holde saken varm, sist ved sin anbefaling til ministrene i 2006[9]. Den er bakgrunnen for at vi nå – i en ny teknologisk situasjon – igjen vurderer om og hvordan det er rom for mulige initiativ.

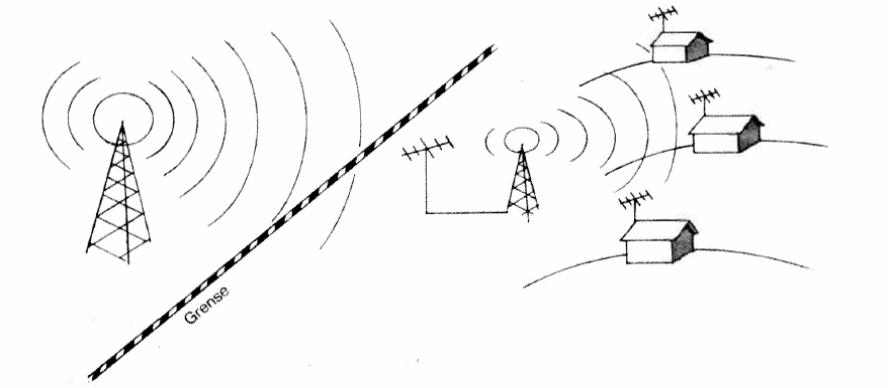
6 NU 1983: 12 Nabolands-tv i kabel
7 Se f.eks den norske utredning Nabolands-tv i kabel, NOU 1984:25
8 Rapport fra Nordisk ministerråd til de nordiske statsministre februar 1994
9 Nordisk råd rek 24.2006

Videresending – ulike varianter

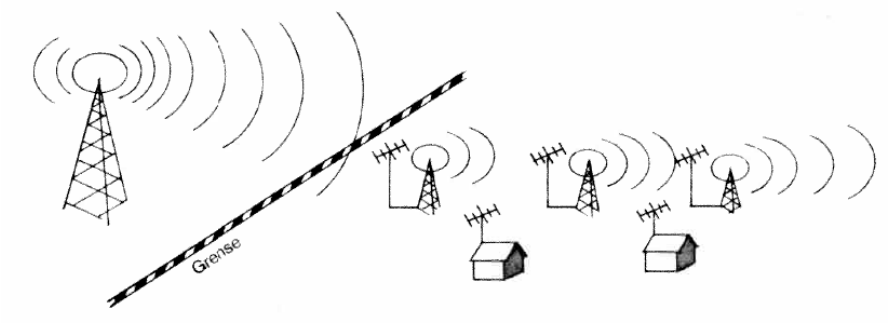
La oss se litt på de ulike variantene av sending og spesielt videresending, som er aktuelle. Jeg anvender illustrasjonene fra den nordiske utredningen av 1984, fordi de fortsatt er relevante.



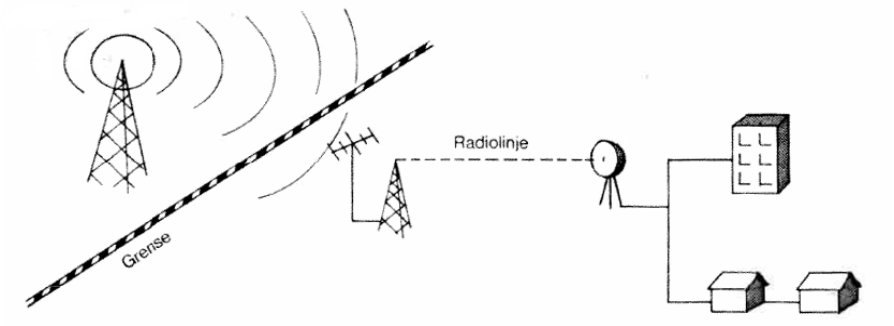
Dette er klassikeren – samtidig og uendret videresending av signaler som krysser grensen, fanges opp og distribueres i kabel til husholdningene.



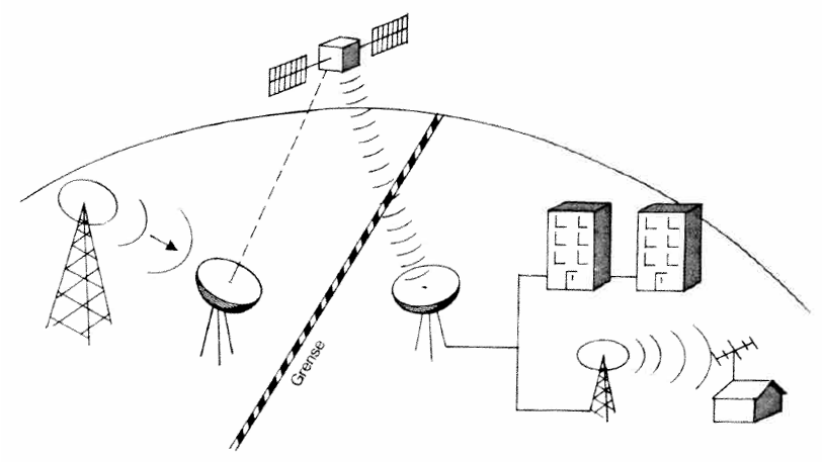
En annen variant, som også er klassisk men langt mindre utbredt, er denne – her fanges signalene opp på andre siden av grensen, og sendes videre over eteren ved hjelp av omformere. Det nye i dagens situasjon er at slik spredning over eter også kan skje i digital form – noe som utvider kapasiteten betydelig (en analog tv-kanal kan romme 6-7 digitale kanaler).



En variant er denne, hvor omformere, såkalte «slavesendere», mater hverandre.

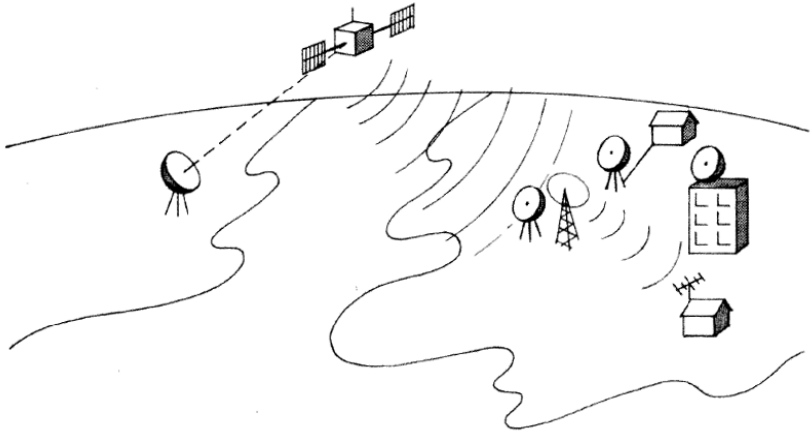


Det hender også at de signalene som fanges opp på andre siden av grensen, føres videre frem til et nytt punkt hvor de så distribueres i et kabelanlegg, slik det her er vist. De kan også ende opp i ny sender eller omformer. Dette benevnes «langdistanse-fremføring». Omformeren kan enten sende på vanlige kringkastingsfrekvenser, eller ved såkalte mikrobølger, og enten i analog eller digital form.



Radiolinjen kan erstattes av en satellitt – slik som vist her; prinsippet er det samme så lenge satellitten kun anvendes til å transportere programmet fra det sted signalet plukkes opp, og frem til kabelanlegget eller omformeren. Rettslig sett skjer det her to ting: det ene er selve langdistanse-fremføringen, det andre er spredningen til husholdningene. Det er denne siste spredningen som i dette tilfelle er opphavsrettslig relevant.

I denne skissen skjer oppsendingen til satellitten i senderlandet. Parallellen til langdistanseoverføring med radiolinje blir bare fullstendig dersom oppsending til satellitten skjer i mottaker-landet – noe som skjer i Norge, hvor TV-signalene bringes fra området nær grensen til Sverige, og overføres med satellitt til videresprednin g i kabelanlegg på Sør- og Vestlandet.



Jeg nevnte at man for 25 år siden opererte med to typer satellitter. Det var *kommunikasjonssattelitter*, med svakere signaler som det trengtes store paraboler for å ta imot, og *direktesendende satellitter* med stor signalstyrke som kunne tas imot med mindre paraboler av individuelle husstander. Etter hvert har utviklingen gått dit at selv svake signaler kan tas imot direkte med relativt små paraboler; *kommunikasjonssatellittene er blitt direktesendende*.

Sending med satellitt direkte til husstandene er rettslig sett det samme som jordbunden kringkasting. Med dagens digitale teknikk kan man både ved satellittsendinger og i jordbundne sendinger kontrollere tilgangen til kanalene. På mange vis er de nye, digitale bakkenettene dermed en slags «kabel i luften».

Som vist på denne figuren, kan satellittens signaler både mate omformere (for eksempel for å betjene områder hvor signalene ikke når fram, såkalt satellitt-skygge) eller bli videresendt i kabelanlegg, samtidig som de kan mottas direkte av husholdninger. Det er fullt mulig å la nabolandets (bakkesendte) TV-signaler bli sendt til opp satellitten for direkte distribusjon i nabolandet, og ikke bare anvende den som middel til langdistanseoverføring.

Dagens satellittsendinger av nordiske allmennkringkastere i Øst-Norden kan teknisk sett også mottas både på Færøyane og i Island med relativt enkelt utstyr, og gi grunnlag for videresending der. For signaloverføring til Grønland kreves særskilt utstyr.

Rettslige problemstillinger

Noen offentligrettslige spørsmål

De rettslige problemstillinger vi møter når vi skal forsøke å øke nabolandsspredningen, er av flere slag. Den første «buketten» er av *offentligrettslig* karakter, jeg nevner det her, uten å gå nevneverdig inn på spørsmålene. I kringkastingsloven kan spørsmålene for eksempel gjelde frekvens-tildeling for omformere, noe som også vil gjelde etter telelovgivningen. Dette er spørsmål som må løses nasjonalt. Et eget spørsmål gjelder såkalt «must carry»-regler – lovpålagte forpliktelser for kabel-operatørene til å videresende visse programmer. Om dette noe mer nedenfor.

Noe mer fokus har det vært på spørsmål om erstatning og straff som følge av *innholdet* i programmer: kan man bli straffet i Norge for en injurie som inngår i et program fra Sveriges Televisjon? Etter den såkalte «senderlandsfilosofien» skulle svaret være nei: slike spørsmål avgjøres i senderlandet etter senderlandets rett. Det har likevel skjedd at Sveriges Television er blitt gjort erstatningsansvarlig i Norge for innholdet av en av sine sendinger som ble

videresendt i kabel i Norge. Saken var imidlertid meget spesiell, bl.a. fordi det aktuelle program ble reklamert for av SVT i Norge før sending.

Noe stort problem har dette imidlertid aldri vært i praksis. Men vil man være garantert at «senderlandsfilosofien» legges til grunn, kreves en mellomstatlig, internordisk overenskomst. (Det samme prinsipp ligger for øvrig til grunn for EU's relevante direktiver om fjernsyn over landegrensene, men er meg bekjent ikke direkte kommet til bindende til uttrykk i noe dokument).

I en Nordsat-sammenheng – hvor alle programmer skulle nå alle etter mellomstatlig overenskomst – var dette en forutsetning. Dette adskiller det formaliserte samarbeidet fra vår problemstilling i dag – hvor videresending i hovedsak skjer uten statlig medvirkning, som oftest i privat regi.

Utfordringene ved videresending av nabolandsprogram har i størst grad vært knyttet til spørsmål av privatrettslig karakter, og da først og fremst til opphavsrett.

Opphavsrettslige utgangspunkter

Utgangspunktene er først og fremst definert ved det faktum at alle de nordiske land er tilsluttet, og dermed bundet av, det rammeverk som er fastsatt i internasjonale traktater og avtaler.

For alle spørsmål gjelder dermed at løsningene må finnes innen de rammene som er lagt i traktatene om opphavsrett i WIPO, Verdensorganisasjonen for immaterialrett. Den viktigste av disse er den såkalte Bern-konvensjonen om vern av kunstneriske og litterære verk, og senere internasjonale avtaler, bl.a. TRIPs – som er immaterialretts-delen av WTO-avtalen fra 1994. Senere WIPO-traktater fra 1996 gjelder opphavsmenn, og utøvende kunstnere og produsenter i fonogrammer.en viktig konvensjon i vår sammenheng er også Roma-konvensjonen til beskyttelse utøvende kunstnere, fonogramprodusenter og kringkastere fra 1961. Et sentralt moment her er at Roma-konensjonen ikke gjelder ikke kringkasting ved tråd – dvs ulike former for sending og videresending i kabel.

Ut over dette har EU gjennom 1990-tallet og frem til 2001 vedtatt en rekke relevante direktiver som også gjelder for Island og Norge gjennom EØS-avtalen. Så også her er de nordiske land underlagt samme rettslige regime – et regime som vi sin tid hadde stor innflytelse på. Det hadde sin bakgrunn bl.a. i Nordsat-prosjektet; der var det jo knapt noen problemstilling knyttet til bruk av satellitt – eller videresending – som ikke var utredet. Erfaringene fra samarbeidet kom til å prege arbeidet i europarådet, og også flere av EU-direktivene. Det er i dette forum verken nødvendig eller ønskelig å gå inn i detaljene – la oss holde oss til hovedlinjene.

Det første utgangspunkt jeg vil nevne er følgende: Kringkasting, eller annen overføring av program til allmennheten ved tråd eller trådløst, er en *eksklusiv rett for opphavsmannen*. Det vil si at den opprinnelige sending – som alltid vil være en sending til allmennheten – må klareres med rettighetshaverne. Den som forestår sendingen må erverve de nødvendige rettigheterne.

Dersom videresendingen i kabel skjer til en allmennhet, kreves det også tillatelse fra rettighetshaverne, dvs fra opphavsmenn, utøvere og fra den opprinnelige kringkaster. Det er visse ulikheter mellom de nordiske land hvor grensene trekkes for når videresendingen skjer til en allmennhet. Som eksempel kan nevnes at det i Norge er fastsatt en grense – etter voldgift – på 25 husholdninger. Videresending over eter – dvs. trådløst – vil alltid være til en allmennhet – og krever altså alltid klarering.

Så kan man spørre seg: hvorfor kan ikke det opprinnelige sendeselskap allerede ved utsendelsen skaffe seg rettighetene til viderespredning?

I prinsippet er det intet i veien for dette. Det er også det som skjer i de fleste kommersielle kanaler: de kjøper rettigheter for det territoriet de vil sende til, med unntak for videresendingsrett for musikk, som må klareres i det land viderespredningen skjer etter de ordninger som har vært gjeldende fram til i dag.

Når det i realiteten er uaktuelt for *allmennkringkasterne* å sikre seg *videresendingsrett*, er det ikke minst fordi det vil være forbundet med betydelig økte kostnader å klarere rettigheter for inntil 20 millioner flere mottakere enn de i dag gjør. Det er også tvilsomt om attraktive program vil være tilgjengelige under en slik forutsetning – mange produsenter ønsker å selge til de enkelte land separat. I tillegg kommer det faktum at noen allmennkringkastere – som NRK – erverver senderettigheter ved såkalt avtale-lisens (se nedenfor). En slik lov-støttet ordning for klarering av senderettigheter gjelder bare innen landets eget territorium.

For våre formål er det, slik jeg ser det, i dag som den gang de første utredningene ble foretatt, slik at *løsningene må søkes i mottakerlandet*.

Løsninger i mottakerlandet

I den videre diskusjon holder jeg meg stadig til *samtidig og uendret* viderespredning – mao. ikke den type spredning som skjer i det svensk-finske samarbeid hvor det er utvalgte deler av de nasjonalt sendte programmene som spres i nabolandet. For disse sendingene skjer det en klarering for de aktuelle programmene.

Det spørsmålet som den nordiske utredning svarte på i 1984 var: hvilken lovgivning kan og bør vi ha for å legge til rette for enkel klarering av rettig-

hetene, slik at videresending skjer? Følgende alternativer for tilrettelegging for viderespredning, gjennom lovgivningstiltak i mottakerlandet, ble lagt fram:

1. Tvangslisenser (eventuelt med nemnd) – dvs. at lovgiver ga bestemmelser som sikret retten til videresending – event. med en mend som kunne treffe avgjørelser om vederlagets størrelse. De internasjonale avtalene og traktatene åpner for muligheten for tvangsløsninger når det gjelder opphavsmenn, utøvere og produsenter, både i kabel og til bruk av omformere/sendere over eter – når det gjelder kringkasterne kan de ikke tvinges til å akseptere videresending i bakkenett eller med satellitt.

2. Avtalelisenser (se nedenfor) – event. supplert med bestemmelser om mekling, eventuelt tvungen voldgift.

Av flere grunner har ingen av de nordiske land valgt direkte tvangs-løsninger, men har innført bestemmelser om såkalt *avtalelisens* for klarering av rettigheter for videresending. Det var også forslaget i den nordiske utredningen av 1984. Avtalelisens innebærer at den som skal stå for videresendingen – oftest kabel-eieren – kan sikre rettighetene ved å inngå avtale med en organisasjon i mottakerlandet som representerer en vesentlig del av rettighetshaverne i landet til den type verk som er aktuelle de aktuelle programmer. Denne avtalen gis ved lov virkning også for ikke-representerte rettighetshavere. Dette gir enkel klarering – og vederlag til rettighetshaverne.

I enkelte av våre land er det gitt regler om tvungen mekling, og dels for at partene kan bringe spørsmål om videresending (og vederlag) inn for avgjørelse i en egen nemnd dersom forhandlin gene strander. I noen land har denne nemnda mulighet for å treffe bindende avgjørelse om viderespredningen i kabel.

I alle de nordiske land har de forskjellige rettighetshavergrupper dannet organisasjoner som på deres vegne kan inngå avtaler om videresendinger av kringkastingsprogrammer. Disse organisiasjonene var etablert før EU i 1995 bestemte at videresedningsrettigheter måtte forvaltes gjennom en felles-organisasjon. Avtaler som utløser avtalelisens lisens kan inngås for videresending både i kabel og i eter – dvs også for distribusjon i digitale bakkenett.

For *kringkasternes rett* til sine sendinger (den såkalte signalretten) gjelder imidlertid ingen avtalelisens-ordning. Kringkastings-(rundradio)selskapene må derfor som utgangspunkt godkjenne videresendingen, uansett måten den skjer på. Når det gjelder videresending i *kabel*, er det imidlertid også for kringkasternes rettigheter åpning for avgjørelse ved tvang – her er rettssituasjonen noe ulik i de nordiske land.

Som en følge av bestemmelsene i Roma-konvensjonen kan imidlertid ikke kringkasterne tvinges til å akseptere *trådløs* videreskredning, dvs videresending ved bruk av omformer eller ved digitalt bakkenett.

Tidligere var kringkastingsselskapene svært restriktive mht til å inngå avtaler om trådløs videresendning. Noe av bakgrunnen for dette var nok holdningen til programleverandører til de opprinnelige sendingene. De var negative til at selskapene skulle åpne opp for en type videresending de ikke var tvunget til å akseptere. Her har situasjonen utviklet seg raskt og i positiv retning mht. muligheter for videresending. Som vi skal høre i neste foredrag er sendeselskapene innstilt på å inngå avtaler når det gjelder egne rettigheter, og sa slik senderettighetene for øvrig bli klarert gjennom de etablerte ordningene.

For å tydeliggjøre mitt poeng, kan vi vende tilbake til fig 7. og 8 om *langdistansefremføring*: fremføringen fra mottakelsen av signalet og frem til kabelanlegget er opphavsrettslig irrelevant – det som må klareres er videresendingen i kabelanlegget. Det gjelder også dersom en bruker en satellitt, såfremt det ikke skjer en (samtidig) sending til enkelt-husstander. Dersom også enkelthusstander skal kunne motta satellittsignalene – noe som er fullt mulig å oppnå – må imidlertid bruken av satellitt klareres (av satellittoperatøren) i mottakerlandet både med den opprinnelige kringkaster, og rettighetshaverorganisasjonen i mottakerlandet.

(Langdistanse-fremføring vil for øvrig for alle praktiske formål alltid resultere i en videresending til en allmennhet – ellers vil det ikke være økonomi i et slikt opplegg. Økonomisk støtte til fremføring av signaler til områder som ikke ellers kan bære kostnader, har vært pekt på som en mulighet for å øke tilgangen, men er meg bekjent aldri realisert).

«Must Carry»-forpliktelser

En løsning for å sikre videresending av nabolands-program som er viktig i diskusjonen, og som finnes i kringkastingslovgivningen i noen land, er en forpliktelse for kabel-eiere til å videresende visse program-såkalt «***must-carry***»-bestemmelse. Dette er en form for ekspropriasjon av kapasitet i kabelen, og finnes hos flertallet av landene for de nasjonale allmennkringkastere.

Men dette er en løsning som også har møtt motstand. Ett argument er at man ikke kan pålegge noen å videresende et program hvis man ikke også kan garantere at rettighetene kan klareres. Ett annet er at en must-carry-bestemmelse som skulle omfatte alle nabolands-programmene ville utgjøre et for omfattende inngrep. Enkelte land har hjemmel for å pålegge videresending som går ut over det som rent faktisk er utnyttet. Vi skal senere i dag få beskrevet at

det ved konsesjonstildelinger for distribusjon av digitalt bakkenett er sikret en viss kapasitet for videresending.

Oppsummering

Denne gjennomgangen har tatt sikte på gi de rettslige utgangspunktene. Etter min mening er de nær de samme som i 1984. Den utvikling som har skjedd har befestet rettighethavernes posisjon i europeisk lovgivning, og har ryddet opp i en del forhold som gjelder satellitt og kabel. De nordiske lands rettslige ordninger er vel tilpasset de internasjonale krav.

Men om utgangspunktene rettslig sett i prinsipp er de samme, har det jo på det teknologiske området skjedd en revolusjon, som har gitt økte muligheter til spredning av nabolands-program.

Min konklusjon er at: *Systemer for rettighetsklarering for videresending er på plass – hvis de ønskes brukt.*

INFORMASJON I INFORMASJONSRETTEN[1]

Jon Bing

Dristig og ambisiøs

Henrik Udsens avhandling *De informationsretlige grundsætninger* er både en dristig og ambisiøs avhandling. Den er dristig fordi den spenner over flere av informasjonsrettens mer spesialiserte emner, og den er ambisiøs fordi den søker å se sammenheng mellom disse emnene. Naturligvis gjør dette også avhandlingen rik – her er det noe for enhver som interesserer seg for informasjonsrett eller noen av de emner som Udsen regner inn under denne samlebetegnelsen, og det ligger på en måte i fremstillingens grunnleggende forutsetninger at forfatteren engasjerer enhver leser i en dialog med boken. Fordi fremstillingen er bred, og fordi den – spesielt i kapittel 7 («Privat brug») og 8 («Konsumption»)[2] – er dyp, vil det være lett å finne detaljer man vil ønske å kommentere.

Internasjonalt finnes det ikke bare i bruk uttrykk som svarer til «informasjonrett» som en upresis samlebetegnelse, det har også vært diskusjoner om man kan rettferdiggjøre å hevde at informasjonsrett er en egen «disiplin», og i så fall hva som skulle tjene som karakteristika. Jeg har selv i beskjeden grad bidratt til denne diskusjonen (og forfatteren nevner sjenerøst dette bidrag), men den gjennomgang forfatteren har (særlig s 51-52) er overraskende summarisk. Den første boken som man kan hevde pretenderte å presentere et informasjonsrettslig perspektiv var Roy N Freed *Materials and Cases on Computers and Law* (Freed, Boston 1968). En annen tidlig bok var Robert P Bigelow *Computers and the Law: An Introductory Handbook* (Standing Committee on Law and Technology, American Bar Association 1968). Den første europeiske fremstillingen var antakelig Colin Tapper *Computers and the Law* (Weidenfeld and Nocolson, London 1973). Men viktigere for de nordiske land var selvfølgelig Peter Seipels doktoravhandling *Computing law: perspectives on a new legal discipline* (Liber Förlag, Stockholm 1977). Denne avhandlingen argumenterer også for – som tittelen indikerer – at «computing law»

1 Innlegg holdt som opponent ved Henrik Udsens doktordisputas, Københavns universitet, 28.august 2009.

2 I kapitteloverskriften bruker forfatteren den besynderlige, men tradisjonelle stavemåten «konsumpsjon». Ellers i avhandlingen bruker forfatteren selv fornuftigvis formen «konsumsjon», det synes som i «konsumpsjon» eller med få unntak bare brukes i sitater.

er en egen juridisk disiplin, og det fremstår kanskje som noe overraskende at forfatteren ikke trekker denne frem, og kanskje også at han ikke sammenligner den angivelse av hva som skal være «computing law» med sitt eget noe avvikende (og kanskje mer hensiktsmessige) syn på hva som omfattes av informasjonsretten. Når man ser hen til at avhandlingene skilles av over tretti år og dramatiske teknologiske sprang symbolisert av slike ting som lanseringen av den personlige datamaskin (1982) og utviklingen av World Wide Web (1990), bør man ikke overraskes av en slik forskjell. I dag er det selvsagt Mads Bryde Andersens monumentale *IT-retten* (Gjellerup, København 2005) som med sine over 1000 sider overskygger alt annet som er skrevet i Norden – en fremstilling som Udsen også gjør god bruk av i sin avhandling.

Jeg har alltid hatt en viss uvilje mot opposisjoner som unnlater å ta opp avhandlingens innholdsmessige vektige sider, og i stedet tar opp spørsmål om avgrensning, disposisjon og andre mer formelle sider. Likevel vil jeg i dette bidraget nettopp konsentrere meg om en av forutsetningene for avhandlingen, nemlig begrepet 'informasjon'.

Definisjonen av informasjon

I en avhandling som omhandler informasjonsrettslige grunnsetninger vil nødvendigvis begrepet 'informasjon' være helt grunnleggende. Nettopp fordi selve ordet inngår i tittelen, ville man vente at ordet korresponderte til et velfundert vitenskapelig begrep. Som forfatteren understreker (s 33) finnes det mange definisjoner av begrepet 'informasjon* -- «næsten lige mange definitioner … som der findes afhandlinger om emnet». Det er nok imidlertid en overdrivelse. Det finnes skoler som samler seg om bestemte definisjoner, gjerne knyttet til ulike disipliner – for «informasjon» er en term som brukes innenfor nokså ulike disipliner som f eks informatikk, telekommunikasjon, psykologi, medievitenskap osv. Forfatteren nøyer seg stort sett med en henvisning til leksikonet *IT-lex* (2001), selv om det gis en summarisk oversikt over en del faglitteratur (s 35) og diskusjoner i tidligere juridisk litteratur (s 36).

Jeg savner nok en nærmere diskusjon av dette grunnleggende begrepet. Jeg tror fremstillingen hadde tjent på en slik avklaring, og vil forsøke å begrunne det nedenfor. Det finnes gode, interdisiplinære fremstillinger av begrepet 'informasjon' – forfatteren smigrer meg ved å henvise til min egen doktorgradsavhandling fra 1982,[3] denne fremstillingen står i særlig gjeld til Ronald Stamper *Information.*[4] Men det finnes mange andre, og sikkert bedre, fremstil-

3 *Rettslige kommunikasjonsprosesser,* Universitetsforlaget, Oslo 1982, se særlig s 66-69).
4 *Information in Business and Administrative Systems,* BT Batsford, London 1973.

linger. Det kunne vært nærliggende å ta opp spørsmålet om det finnes et eget *rettsvitenskaplig* informasjonsbegrep, eller om man i rettsvitenskapen, og da spesielt i informasjonsretten, benytter det samme begrep som er utviklet innen en annen disiplin. Slik jeg forstår forfatteren, bygger han på at begrepet er det samme som innen informatikken mer generelt.

Forfatteren bygger opp definisjonen av informasjon (s 35-36) med å ta utgangspunkt i begrepet 'data'. Dette defineres (s 35) som «ethvert fenomen, der kan erkendes og bearbejdes i den menneskelige hjerne». Dermed kan 'informasjon' defineres som «det meningsindhold, der fremstår for den, der tolker de pågældende data». Dette forutsetter, som forfatteren fremholder (s 38), et felles språk som gjør at avsender (som innkoder meningsinnhold i data, f eks en tekst) og mottakeren (som avkoder meningsinnholdet fra den samme teksten) deler et språk, denne felles bakgrunn gjør det mulig å kommunisere. Slik gjør forfatteren et tradisjonelt skille mellom syntaks og semantikk. Forfatteren benytter seg imidlertid ikke direkte av det tredje tradisjonelle elementet, nemlig 'tegn'. Et tegn defineres som et symbol som alene eller sammen med andre symboler utgjør data, dvs at tegnene er føyd sammen i henhold til en gyldig syntaks, det språk som kommuniseres frem til en mottaker og forstås av denne som et meningsinnhold. Jeg tror forfatteren kunne også gjort god nytte av begrepet 'tegn' i sine analyser.

Forfatteren henviser til arbeider som belyser begrepet informasjon, bl a til den spennende, norske språkpsykologen Ragnar Rommetveit.[5] Nøyaktig på det sted i Rommetveits bok som forfatteren henviser til, gjør Rommetveit en avgjørende sondring mellom «eit naturleg teikn» og kommunikasjonshandlinger, illustrert bl a med et eksempel:

> *«Eg kan gå meg vill i jungelen – og eg trør sund kvister der eg fer fram i ørske. Eit leitemannskap kan finna dei sundbrotne kvistane, og kvistane 'tyder på' at eg gått i ei viss lei. Dei formidlar informasjon om mi ferd, men ingen bodskap.»*

Denne distinksjonen ville Udsen kunne ha utnyttet i sin diskusjon om at informasjon må være skapt (s 102). Sondringen mellom budskap og naturlig forekommende tegn ville ha klarlagt at de naturlig forekommende tegn ikke er «data» formet innenfor rammene av en gyldig syntaks, de representerer rett og slett ikke et budskap.

Man kunne kanskje også reise spørsmålet om ikke et *kommunikasjonsperspektiv* hensiktsmessig ville supplert begrepsapparatet. Forholdet mellom

5 Ragnar Rommetveit *Språk, tanke og kommunikasjon,* Universitetsforlaget 1979.

«data» og «informasjon» impliserer en kommunikasjon fra en «avsender» til en «mottaker» som tolker data. Men 'data' er – slik jeg forstår det – alltid menneskeskapt, det er tegn som er føyd sammen til et budskap i henhold til en gyldig syntaks. Imidlertid vil et menneske også kunne iaktta naturlige fenomen, som Rommetveits istykkertrådte kvister. På grunnlag av denne observasjonen, kan det dannes en forståelse som observatøren senere kan formidle videre som data. Dermed kan det i alle fall være hensiktsmessig å sondre mellom den «primære» innsamlingen av informasjon, og den derpå følgende videre kommunikasjon av egen forståelse i form av data. Det meste vi formidler videre, er for så vidt rapporter om vår egen forståelse av data vi har mottatt, bearbeidet i våre tanker og dermed mener å kunne formidle videre med den tilleggsverdi denne bearbeidelsen representerer. Men naturligvis finnes det også en andel originære observasjoner – vi ser og hører hva som skjer rundt oss, vi føler en varm bris og klapper en myk katt. Slik samler vi primær informasjon som vi så kan formidle videre som data, og skape informasjon hos mottakere som slik kan forstå våre opplevelser. Også rettslig kan det være meningsfullt å sondre mellom originær innsamling av informasjon og videreformidling, f eks i forfatterens diskusjon av forretningshemmeligheter eller om(?) fotografier tatt i hemmelighet, hvor det kanskje ikke er selve fotograferingen som rettslig sett er problematisk, men videreformidlingen av fotografiet, f eks til et ukeblad for publisering.

Erkjennelse av informasjon

Noen av problemene med begrepene avdekker forfatteren selv i avsnittet om erkjennelse (s 45). Ettersom informasjon er definert som det meningsinnhold som oppstår ved tolkning av data, blir det nokså opplagt at «[e]rkendelse af information er et vanskelig begrep» (s 45), ettersom erkjennelsen er bygget inn som et kriterium i selve definisjonen av informasjon. Et annet problem avdekkes i innledningen av avsnittet:

> *«Modtagerens erkendelse afslutter den proces, hvor data opfanges, bearbejdes og forstås i den menneskelige hjernen(eller af en computer).»*

Det er tillegget i parentes som er problematisk. Slik jeg oppfatter det, modifiserer dette det grunnleggende begrepet 'informasjon' slik definisjonen er gjengitt ovenfor, hvor 'informasjon' er begrenset til forståelse av data i «i den menneskelige hjerne». Hvis man også tar med bearbeidelse av data i en datamaskin som «forståelse», må man tenke gjennom hva slags tolkning en maskin gjør av data. Jeg har en gang hørt John McCarthy, en av de sentrale pionerene innen kunnskapsbaserte systemer («kunstig intelligens») argumentere for at

en termostat var «intelligent». Mennesker opplever endringer i temperaturen i et rom og tolker det som at det blir «varmere» eller «kaldere». Termostaten registrerer temperatursvigninger og tolker det som at en nål skal flyttes opp eller ned over en skala.

Jeg mener ikke å antyde at Udsen har samme ekstreme syn på maskinintelligens som McCarthy. Men det er åpenbart at tolkingen av data – semantikken – vil være svært forskjellig mellom mennesker og maskiner. Skriver jeg et ord på et tastatur, vises ordet på skjermen og en venn som ser over skulderen, vil lese ordet og forstå det – f eks ordet «barn». Datamaskinen har mottatt data i form av impulser fra tastaturet, og tekstbehandlingsprogrammet vil tolke dem som instrukser om å vise bestemte og forhåndsdefinerte tegn på skjermen, tegnene «b», «a», «r» og «n» uten ordmellomrom. Dette er en antydning av den «forståelse» maskinen har av ordet er helt annerledes enn den tolkning min venn som leser på skjermen, vil ha av dette samme enkle ordet.

Det er forholdsvis enkelt å påvise at forfatteren ikke bruker termen «informasjon» konsistent. Nå er ordet «informasjon» en del av hverdagsspråket og brukes i mange sammenheng. Det er derfor høyst forståelig at det i praksis vil være vanskelig å fastholde den definerte betydningen, spesielt er det vanskelig å fastholde sondringen mellom 'data' og 'informasjon'. For eksempel vil et uttrykk som «informasjonsbehandling» være problematisk. Ettersom informasjon er «forståelse», fortrinnsvis i den menneskelige hjerne, kan informasjonsbehandling bare foregå ett sted, nemlig i hjernen. Men til daglig snakkes det om at datamaskiner behandler informasjon, og i en avhandling om informasjonsrett, ville det være nær umulig å unnlate bruk av ordet i den dagligdagse og upresise betydningen. Muligens er det nettopp ønsket om å kunne bruke et uttrykk som «informasjonsbehandling» som har forledet forfatteren til å ta med «computer» i parentesen i sitatet ovenfor. Nordiske språk har – i motsetning til engelsk – et ord som er nøytralt i forhold til «data» og «informasjon», nemlig «opplysning». Også forfatteren bruker dette av og til (f eks s 40, 125), men jeg tror denne muligheten kunne vært brukt oftere.

Jeg mener altså at forfatteren har valgt en riktig og hensiktsmessig definisjon av begrepet 'informasjon', men at termen ikke brukes konsistent i avhandlingen. Imidlertid mener jeg også at et krav til absolutt konsistens ville være helt urimelig fordi «informasjon» inngår i dagligspråket, og det ville virke stivt og konstruert å unngå den bruken som dagligspråket har alminneliggjort. Det er høyst forståelig at man snakker om «informasjonsbehandling», selv om det strengt tatt ikke er korrekt, for det korrekte uttrykket – «databehandling» – faktisk virker litt alderdommelig. Der hvor det derfor ikke virker villedende, kan man falle tilbake på den upresise dagligtalen, det skaper ikke misforståelser. Men hvor det er nødvendig for analysen, må definisjonen opprettholdes.

Informasjon og medieavhengighet

Forfatteren diskuterer informasjonens særlige karakteristika, og tar opp i et underavsnitt «Medieafhengighet» (s 36). Her understrekes det at informasjonen alltid er knyttet til et medium, og det heter bl a:

> *«Denne medieafhengighet bevirker, at information altid optræder i en kombination af noget materielt (mediet) og noget immaterielt (informationen).»*

Som eksempler på medier nevnes i avsnittet papir, «lyd på en CD», lyd og «impulser i hjernen».

Etter diskusjonen ovenfor, ser en lett at dette er en forklaring av *datas*, ikke informasjonens medieavhengighet. Informasjon er forståelse, og kan bare oppstå i den menneskelige hjerne slik begrepet er definert. Data, derimot, må være representert på et medium – som tegn på et papir, som fordypninger på en optisk plate («lyd» blir resultatet når platen avspilles på egnet utstyr) osv. Den samme informasjonen kan formidles på ulike måter, et foredrag kringkastet i radio vil gi lytteren den samme informasjon som om han eller hun leste foredraget i en bok. Ved å knytte medieavhengigheten til data snarere enn informasjon, ville forfatteren unngå en del åpenbare problemer. Det grunnleggende nevnes allerede i samme avsnitt, hvor det hevdes nokså bastant at:

> *«Mediet kan uden videre placeres inden for de regler, som regulerer fysiske genstande, mens det ofte er vanskeligt at avklare, hvordan disse regler skal tilpasses informationsfaktummet.»*

Dette er åpenbart å gå for langt, forfatteren har jo selv noen linjer lenger opp gitt som eksempel på medium, «den ikke-udtalte idé [bæres] af impulser i hjernen». Det er langt fra åpenbart at hjernen, som her er mediet, uten videre reguleres av de bestemmelser som kommer til anvendelse på løsøregjenstander som papirark eller optiske plater. Det ville derfor lettet analysen i dette avsnittet, så vel som i andre passasjer hvor forholdet mellom «medium» og «informasjon» er sentralt, om forfatteren hadde knyttet analysen til «data» snarere enn «informasjon». Forfatteren får rett og slett ikke utnyttet fordelene av den terminologien han selv har etablert.

Dette ser man også i avsnitt 2.3.2 om informasjonens medieavhengighet. Her retter forfatteren (s 38) fokus mot den «fleksible information», en egenskap som «tillader informationen at springe fra et medium til et andet». Her får forfatteren behov for å skille ut informasjon der lagringen kan skje i den menneskelige hjerne, informasjon som formidles med lydbølger, som en flyktig

representasjon.[6] Hvis denne diskusjonen var blitt knyttet til «data» snarere enn «informasjon», ville den blitt mye enklere – og kanskje også mer fruktbar. Overføring av data fra ett medium til et annet, også ved overføring over tråd som et tog av elektriske impulser (en vel så flyktig representasjon som lydbølger) er viktig i informasjonsretten, ikke minst i immaterialretten. Det er ingen grunn til å blande inn den menneskelige forståelse i dette – det er data som kopieres og formidles, og den fleksibiliteten forfatteren omtaler, burde vært knyttet til data, ikke informasjon. Det forhindrer selvsagt ikke at den forståelse et menneske har i sin hjerne (informasjon) kan representeres på ulike måter som data, forståelsen kan formuleres som ord, ordene kan skrives, synges, kringkastes osv.

Forfatteren bruker også av og til uttrykket «informationsprodukt» (f eks s 360). Det er ikke helt lett å se hva dette ordet nærmere skal bety, det kan bety et produkt som er blitt til ved utnyttelse av vernet «informasjon» (f eks en patentert oppfinnelse eller en forretningshemmelighet), men det kan også bety omtrent det samme som et «databærende medium», hvor det er informasjon formidlet gjennom produktet som begrunner verdien snarere enn mediet selv.

Informasjonstyper

Forfatteren skiller mellom *typer av informasjon,* hvor sondringen gjøres på grunnlag av en karakteristikk av meningen. I pkt 2.3.1 (s 39) sondres det mellom operasjonell og emosjonell informasjon, en sondring forfatteren låner fra Mads Bryde Andersen.[7] Den operasjonelle informasjon er egnet til å danne et beslutningsgrunnlag, mens den emosjonelle informasjon er egnet til å fremkalle følelser.

I forbindelse med diskusjonen av «Ytringsfrihed som indskrænkning i informationsrettighederne» (s 373) behandler forfatteren immaterialretten (s 374), og i han tar opp (s 379) avgrensningskriterier. Her fremhever han innledningsvis at det har betydning hvilken *type* informasjon det er snakk om. Det eksempelet som nevnes er "politiske ytringer og andre ytringer af samfundsmæssig interesse". Dette må være nær sammenfallende med «politiske meningstilkendegivelser mv.» som angis som en informasjonstype i forbindelse

6 Forfatteren tar her også med som eksempel «lyspartikel», det siktes da antakelig til et foton, som alle kvantumpartikler vil fotonet både kunne beskrives som en partikkel og en bølge. Forfatterens ordvalg tar sikker ikke sikte på å ta stilling til kvanteteoretiske spørsmål og utlukke at lys også kan anses som en bølge.

7 "Fragmenter af en informationsretlig grundregulering", Mad Bryde Andersen, Caroline Heide-Jørgensen og Jens Schovsbo (red) *Festskrift til Mogens Koktvedgaard*, Jurist- og Økonomforbundets Forlag, København 2003:5-25.

med noen overordnede betraktninger om de informasjonsrettslige hensyn (s 125). Like ovenfor omtales «visse typer av personopplysninger, særlig de følsomme opplysninger». Her synes det som om sensitive opplysninger er en type underordnet «personopplysninger», som da også må være en type informasjon.

Han nevner også «information [som] anvendes som led i kunstnerisk virke» (s 379). Dette er eksemplene på informasjonstyper som nevnes, og de sammenlignes med et annet kriterium relevant for bruk av bestemmelser om ytringsfrihet, hvorvidt informasjonen har «offentlig interesse» – men dette er altså ikke en informasjonstype, men et kvalitativt forskjellig kriterium.

I diskusjonen av vernet av forretningshemmeligheter og ytringsfrihet (s 383) henviser også forfatteren til «informationstypens betydning», og angir at det først og fremst er informasjon «som har karakter af nyheder eller i øvrig er 'a matter of public concern'» som tillates offentliggjort i henhold til den amerikanske grunnlovs vern av ytringsfriheten.

Mye tyder på at forfatteren ikke har hatt oppmerksomheten rettet mot kvalifikasjonen av «informasjonstyper». Det er ikke angitt noe kriterium for hvordan man skiller mellom ulike typer, men det fremgår av sammenhengen at forfatteren bruker *forståelse* som kriterium. Det finnes naturligvis en nær ubegrenset palett av ulike nyanser i vår forståelse av data, og forfatteren har utnyttet noen nokså enkle sondringer som synes viktige ut fra den aktuelle rettslige kontekst. I forhold til ytringsfriheten, er det naturlig å fremheve politiske ytringer. Det er naturlig å angi personopplysninger som en informasjonstype, og denne kategorien kan ytterligere deles i «trivielle», «sensitive» og «vanlige» personopplysninger.

Det er derfor egentlig ingen innvending at forfatteren ikke behandler informasjonstyper prinsipielt, men lar det være en pragmatisk sondring innenfor ulike områder av informasjonsretten. Men grunnen til at dette er interessant, er spørsmålet om det finnes kriterier for å sondre mellom ulike kategorier eller typer av informasjon som også er rettslig relevante.

Jeg har av og til lekt med tanken om hvorvidt svaret kunne gis av spørsmålet «Hvorfor er noen villig til å *betale* for informasjon» (og da er uttrykket brukt i forfatterens definerte betydning). Men kan tenke seg flere forklaringer.

(1) Ut fra tradisjonelle syn på informasjonssystemer for ledelse, så vil den økonomiske verdien av informasjon produsert av et slikt system være sannsynligheten for at ledelsen på dette grunnlag vil kunne treffe avgjørelser som fører til at bedriften tjener mer, eventuelt sparer utgifter. Dette er, som sagt, den tradisjonelle begrunnelsen for informasjonssystem for ledelsen i bedrifter. (2) Nær beslektet er informasjon som definerer eller begrunner en konkurranseposisjon i markedet, f eks en bedriftshemmelighet. Denne gjør at bedriften

kan produsere en vare eller tjeneste til lavere priser eller med høyere fortjenestemarginer enn konkurrenter. (3) Utdannelse er en informasjonstjeneste, og hvis man er villig til å betale for utdannelse, kan man kanskje anta at dette er begrunnet i en tro på at utdannelsen vil kunne kvalifisere vedkommende til en jobb som gir en høy eller høyere lønn. Men sannsynligvis er det også et betydelig moment av selvrealisering. (4) Informasjon vil ofte være underholding – som teater, musikk, en sportsbegivenhet, en roman osv. Her er det opplevelsen som er sentral, og man er villig til å betale for denne opplevelsen. (5) Nyheter har antakelig i seg selv en verdi, men er villig til å betale for å bli underrettet om hvordan «verden endrer seg». Dette er grelt illustrert av børskurser, som man må betale dyrt for å få i sanntid, men som er gratis tilgjengelig dagen etter. Men det er kanskje heller et eksempel på den første kategorien (ledelsesinformasjon), ettersom sanntidsopplysninger har verdi fordi de kan legges til grunn for beslutninger som kan føre til gevinst eller avgrense tap. Og dermed illustreres at de antydede kategoriene ikke utelukker hverandre, men tvert imot ofte vil overlappe hverandre.

Det finnes sikkert andre kategorier eller typer informasjon. Hensikten har bare vært å illustrere at en typologi faktisk også kunne være rettslig interessant, og at informasjonstyper ikke behøver å være fullt så pragmatisk som Udsen gjør dem.

Det går naturligvis an å kvalifisere «informasjon» på andre måter enn å inndele dem i typer. Det gjør da også forfatteren. Uttrykket «ren information» forekommer første gang s 24, og brukes noen få ganger til, bl a som «ren informationsmængde» (s 260). Igjen synes det vanskelig å skjønne hvorfor denne forsterkningen er nødvendig, men det kan være et tegn på at forfatteren selv innser at han ikke har klart å fastholde den definerte betydningen av 'informasjon', og dermed føler behov for å presisere at det nettopp er i betydningen 'kunnskap' eller 'forståelse' uttrykket blir brukt i de aktuelle sammenhengene.

Informasjonsmengde

En av de termene forfatteren bruker flere steder er «informasjonsmengde». [8] Dette synes å implisere at man kan måle eller kvantifisere «informasjon». Informasjon har forfatteren – jfr ovenfor – definert som «det meningsindhold, der fremstår for den … [som tolker] data».

Åpenbart må det være problematisk å kvantifisere «meningsinnhold». For å si det forsiktig, er det omtrent som å snakke om «en kilo tanker». Informasjon

8 Se f eks s 17, 39, 40, 43,45, 54, 55 osv – det er ingen grunn til å gi en fullstendig liste av alle forekomstene av uttrykket.

er nettopp i slekt med uttrykk som «tanker», «følelser», «ideer» osv – ord som beskriver de kognitive prosesser som skjer i våre hjerner. Det er naturligvis ingen grunn til i denne sammenheng å ta opp diskusjonen om hvordan vi tenker eller lignende spørsmål som diskuteres av f eks psykologer. Vi nøyer oss med å konstatere at den definisjonen av *informasjon* som forfatteren har valgt, viser til kognitive fenomen, og at derfor det å måle en «mengde», er meningsløst.

Det betyr selvsagt ikke at man med andre definisjoner av «informasjon» kunne foreta en kvantifisering. I forbifarten nevner forfatteren Shannons informasjonsteori (s 35), sitert med henvisning til den grunnleggende artikkelen av Shannon og Weaver (1949), en teori som ofte betegnes som «kommunikasjonsteorien». Det kan synes som om Udsen tar teorien til inntekt for sitt eget syn på informasjon. Men egentlig er vel Shannons perspektiv nokså forskjellig.[9] Hans opprinnelige problem var hvordan man best skulle utnytte kapasiteten i smale kommunikasjonskanaler, f eks ved kortbølgesendinger i en krigssituasjon. Han målte sannsynligheten for at ett bestemt tegn fulgte etter et annet og kjent tegn. Hvis sannsynligheten var høy, ville «informasjonsverdien» være lav, og dermed kunne man sløyfe tegnet uten at «informasjon» gikk tapt. Et omtrentlig eksempel illustrerer poenget – er det kjent at det ord som skal formidles har syv bokstaver, og at de fem første er «papeg», vil nesten alle norske språkbrukere skjønne at ordet er «papegøye», noe som betyr at «øye» er redundante tegn som kan sløyfes. Slik fremstår Shannons kommunikasjonsteori som en nærmest rent syntaktisk teori, et alternativ til Udsens semantiske definisjon av «informasjon», og – tror jeg – en teori som ikke er like velegnet som grunnlag for en diskusjon av informasjonsretten. Men denne teorien gjør det meningsfullt å måle informasjon, kanskje også å snakke om «informasjonsmengde», selv om «informasjonsverdi» nok er mer nærliggende.

Immaterialrett og informasjon

I alle fall i to sammenhenger synes det som om forfatteren bruker det definerte uttrykket «informasjon» til å forklare aspekter ved gjeldende immaterialrett. I forbindelse med diskusjonen av konsumsjon av visningsrett, fremholdes at visningsretten først konsumeres «når værket (informationen) er gjort tilgængelig for offentligheden» (s 335). Forholdet til parentesen utdypes ikke i teksten, men det er nærliggende å assosiere forholdet mellom 'data' og 'informasjon' med forholdet mellom 'utførelse' og 'verk' i opphavsretten. Distinksjonene er klarligvis nært beslektet. På den annen side er det sannsynlig at opphavsrettslig teori og praksis gjennom årtier har tilført begrepet 'verk' så mange detaljer og

9 Dette fremheves også av Rommeteveit (1979:181), en annen av de kilder forfatteren viser til.

nyanser at man skal være forsiktig med å anta at det foreligger identitet mellom 'verk' og 'informasjon'. Slik kan heller ikke forfatterens parentes forstås i den sammenheng den forekommer.

Forfatteren omtaler i innledningen til diskusjonen av informasjon om egne ytelser at det ikke er praktiske eksempel på at det har vært nødvendig å informere om egne ytelser i forbindelse «patentbeskyttet information». Det kan vel være fordi det er vanskelig å finne eksempel på at informasjon i seg selv er en oppfinnelse i patentrettens forstand, og dermed kan bli patentbeskyttet. Det nærmeste man komme i europeisk rett er kanskje datamaskinprogrammer, som til tross for at de utelukkes i den europeiske patentkonvensjonen synes å kunne bli patentert.[10] Men programmet er likevel ikke informasjon i forfatterens terminologi, det er en tekst skrevet i et kunstig språk og etter strenge, syntaktiske regler. Nærmere kommer man kanskje i amerikansk rett hvor bl a forretningsmetoder kan patenteres. Jeg velger likevel å tolke forfatteren dit hen at det i uttrykket ikke ligger noen påstand om at informasjon kan patenteres, men at forfatterens oppmerksomhet ikke har vært fullt ut konsentrert om formuleringen.

Unnskyldning

Leseren har sikkert for lengst skjønt at jeg er blitt revet med av avhandlingen, og at jeg – som flere andre – har oppdaget hvor relevant den er for ting jeg er spesielt opptatt av. I dette innlegget har jeg begrenset meg til selve begrepet 'informasjon', som jeg mener er et sentralt begrep ikke bare i informasjonsretten, men i det samfunnet vi lever og virker. Det virker sikker monomant hvordan jeg med dette ene ordet som ønskekvist, søker etter skjulte kilder i forfatterens omfattende verk. Det er selvsagt dypt utrettferdig, fordi dette helt maskerer den store verdi som har skapt min begeistring for avhandlingen. Jeg ber derfor forfatteren ydmykt om unnskyldning for at jeg slik legger avhandlingens verdifulleste sider i skyggen, men takker samtidig for at jeg har fått anledning til å belyse noe som forfatteren og jeg er enige om at er sentralt i informasjonsretten, nemlig selve ordet «informasjon».

10 Jfr Are Stenvik *Patentrett,* Oslo 2006:140-141.

NORSKE FORSLAG OG DEBATTER OM PSEUDONYME HELSEREGISTRE[1]

Herbjørn Andresen

1 Innledning

I et medisinsk behandlingsopplegg må pasienten leve med at det er nødvendig å behandle personopplysninger. Noen opplysninger samles inn fra pasienten selv, mens andre opplysninger oppstår gjennom behandlingsforløpet. En viss trussel mot opplysningenes konfidensialitet er uunngåelig, og risikoene må analyseres, overvåkes og håndteres. Regler om behandling av opplysninger, informasjonssikkerhetstiltak og profesjonsetikken beskytter mot ulegitimert behandling og lagring, og mot tilsiktet misbruk av pasientopplysninger.

Personvernet er også truet når pasientens helseopplysninger brukes utover den medisinske behandlingen som er avtalt, selv om denne bruken kan være legitim og ønskelig. Slik bruk kan man kalle sekundære formål for behandlingen av opplysningene. Temaet for denne artikkelen er en spesiell variant av slike sekundære formål, nemlig de nasjonale helseregistrene. Et register er en tjeneste som omfatter en database, praktisk organisering, og et hjemmelsgrunnlag som definerer ansvarsforhold, plikter til å rapportere til registeret, restriksjoner som gjelder bruken, og så videre. I dagligtale oppfatter man et registers navn som navnet på selve databasen. Organisering og hjemmelsgrunnlag er underforstått.

Registrene har to viktige egenskaper, sett fra et personvernsynspunkt. For det første er de sentraliserte, og inneholder aggregerte data. Pasienters helseopplysninger samles inn fra ulike sykehus eller andre behandlingsinstitusjoner. Prosedyren for å hente inn opplysninger kan enten være basert på elektronisk utveksling, eller papirutskrifter som tastes inn på nytt i det sentrale systemet. Den andre egenskapen er at opplysningene samles inn og behandles for sekun-

1 * Artikkelen er oversatt fra *The Norwegian Policy Debate on Pseudonymous Health Registers*, trykket i Fred, Filipe og Gamboa (red.) *Biomedical Engineering Systems and Technologies: International Joint Conference, BIOSTEC 2008. Funchal, Madeira, Portugal, January 28-31, 2008. Revised Selected Papers*. Springer 2009 s. 413-424. Jeg har lagt oversettelsen nær opp til originalversjonen, men visse detaljer i teksten som forklarer hvilken funksjon enkelte kilder har i norsk samfunn og rettsliv er utelatt fordi de ville være overflødige her. I tillegg er det føyd til noen nye fotnoter

dære formål, som til dels kan ligge fjernt fra det en pasient vil oppfatte som sine umiddelbare interesser og behov. De sekundære formålene kan deles i to hovedgrupper, den ene er overordnet statlig styring, den andre er medisinsk og helsefaglig forskning. Overordnet statlig styring omfatter makronivå beslutningsstøtte og kontroll med finansierings- og refusjonsordninger. Behovet for opplysninger til slike formål er, i hvert fall prinsipielt sett, begrenset og forutberegnlig. Medisinsk og helsefaglig forskning vil også i mange tilfeller ha behov for opplysningstyper som er definert og kjent på forhånd, men i tillegg kan man i en del tilfeller ha nytte av overskuddsinformasjon og opplysninger som fremkommer ved koblinger mellom ulike datakilder. Den fremtidige verdien av oppfinnsom leting i et stort datamateriale er nødvendigvis ukjent.

Regelverk, sikkerhetstiltak og etiske forpliktelser er selvfølgelig minst like påkrevd for registrene som for opplysningene i de behandlingsrettede primære informasjonssystemene. Registrene kan i tillegg være utsatt for press i retning av å utvide de opprinnelige formålene som lå til grunn for etableringen. Tilhengere av strenge regler om personopplysningsvern advarer mot «skråplaneffekter»: Jo mer registrene brukes, jo vanskeligere kan det bli i hvert enkelt tilfelle å si nei til enda et forslag om enda mer utvidet bruk. Slike forslag tjener ofte gode formål, og fremstår i mange tilfeller som den beste og mest skånsomme måten å nå et gitt mål på. Derfor innebærer registrene en fare for uthuling av pasientenes personopplysningsvern over tid.

1.1 Norges historisk gunstige vilkår for helseregistre

Norge etablerte nasjonal personidentifikator relativt tidlig. Fra 1964 begynte Statisk sentralbyrå å tildele et unikt, 11-sifret identifikasjonsnummer til hvert individ. Den opprinnelige hensikten med den nasjonale identifikatoren var å produsere nøyaktig og pålitelig statistikk. Store offentlige virksomheter, som skatte- og trygdeetatene, tok tidlig det nye fødselsnummeret i bruk. Ingen forutså den gang den enorme fremtidige utbredelsen. Da fødselsnummeret ble introdusert, fantes det ingen klar hjemmel som støttet det. Dermed var det heller ingen lett tilgjengelige og klart formulerte begrensninger for bruken.[2]

På grunn av mangelen på tydelige restriksjoner mot bruk av fødselsnummeret i begynnelsen, er det nå nøkkelen til personlige opplysninger i et enormt antall offentlige og private IT-systemer i hele landet, inkludert pasientjournalsystemer og andre behandlingsrettede systemer i helsesektoren. De fleste nordmenn må taste inn (eller fremsi) sitt unike fødselsnummer i en elektronisk

2 Knut Selmer: *Hvem er du: Om systemer for registrering og identifikasjon av personer.* I: Lov og Rett. Årg. 31, s. 311-334 (1992)

innretning (eller til dens menneskelige dørvokter) flere ganger i uken. Den utbredte bruken av fødselsnumre i Norge er en viktig årsak til at vi har gunstige vilkår for nasjonale helseregistre. Den felles identifikatoren brukes i så mange systemer som er viktige for de fleste av oss, at bruksomfanget i seg selv bidrar til å styrke dataenes referansekvalitet. Registre med fødselsnumre som identifikator er teknisk sett egnet til å samle og koble opplysninger om oss fra fødselsmelding til obduksjonsrapport.

De første årene med enormt ekspanderende bruk av fødselsnummeret ble etterfulgt av nærmere tre tiår med forsøk på å sette grenser for bruken. Personopplysningslovens kriterier for når det er tillat å bruke fødselsnummer som identifikator[3] har neppe bidratt nevneverdig til en faktisk begrensning. Likevel oppfatter mange helseforskere en viss tvil om hvorvidt det vil være lov å bruke fødselsnummer for identifisering av forskningsdeltakerne i sine prosjekter. Et helseregister vil ikke kunne gi ut ikke-anonymisert pasientinformasjon til et forskningsprosjekt som ikke kan oppvise tilstrekkelig grunnlag for det.[4]

Selv om fødselsnummeret og høy referansekvalitet i primærsystemene bidrar til gunstige betingelser for helseregistre, har det vært ytret mye bekymring om at rettslige restriksjoner hindrer at potensialet utnyttes fullt ut. Denne situasjonen har medført to parallelle debatter: Den første gjelder balansen mellom personvern og hva som skal være legitim bruk av et helseregister. Den andre debatten gjelder mulighetene for å omgå behovet for å identifisere den enkelte pasient, uten at registeret taper sin nytteverdi.

1.2 De digitale pseudonymers opprinnelse

Et pseudonym er, rent bokstavelig, et «falskt navn». Gjennom historien har pseudonymer vært brukt av forfattere og kunstnere, eller til og med av noe så sjeldent som beskjedne forskere, for å skjule deres virkelige identitet. Ideen om et *digitalt* pseudonym ble først uttrykt i en artikkel av David Chaum. Han lanserte digitale pseudonymer som et middel for å holde individenes identitet

3 «Fødselsnummer og andre entydige identifikasjonsmidler kan bare nyttes i behandlingen når det er saklig behov for sikker identifisering og metoden er nødvendig for å oppnå slik identifisering», lov 14. april 2000 nr. 31 om behandling av personopplysninger, § 12 første ledd

4 Etter at denne artikkelen først kom på trykk har ny helseforskningslov, lov 20. juni 2008 nr. 44 om medisinsk og helsefaglig forskning, trådt i kraft. Den nye loven skulle ikke ha vesentlige følger for innholdet i denne artikkelen

skjult under elektroniske transaksjoner.[5] Det tiltenkte anvendelsesområdet i Chaums artikkel var banktransaksjoner og elektronisk handel. Pseudonymets hensikt var å ikke avsløre hvem som egentlig betalte for varer og tjenester.

I noen etterfølgende artikler utviklet Chaum både metodene og ideene om formål og anvendelsesområder videre. De relativt nye prinsippene for kryptering ved distribusjon av aktørenes offentlige krypteringsnøkler[6] ble foreslått som metode for å tildele et sikkert, kryptografisk pseudonym. For at den person som pseudonymet gjelder skulle kunne kommunisere, og få innsyn i sine egne personopplysninger, kunne en tiltrodd tredjepart forvalte pseudonymene. Formålet ble etter hvert utvidet til å omfatte et nytt paradigme for personopplysningsvern; bruk av teknologiske virkemidler for å gi det enkelte individ kontroll over egne opplysninger.[7] Organisasjoner ville ikke være i stand til å dele data om en person uten at vedkommende praktisk talt utøvde sitt samtykke, som en konkret handling. Ingen ville kunne samle den fullstendige historien over en persons transaksjoner, sparepenger eller gjeld. Den personen pseudonymet gjaldt for, skulle selv sitte med nøkkelen til å reversere det.

Chaums forslag til nytt paradigme for personopplysningsvern innen finans og elektronisk handel synes å ha tapt fullstendig for det gamle paradigmet: Omfattende bruk, underlagt virksomhetenes kontroll, av opplysninger om entydig identifiserte personer. I ettertid ble imidlertid ideen om digitale pseudonymer gjenopplivet innen områdene helseadministrasjon og medisinsk og helsefaglig forskning.

1.3 Pseudonymiseringsprosessen

Prosessen med å generere pseudonymer kan gjennomføres på ulike måter. Den enkleste formen for pseudonymer, brukt gjennom flere tiår i forskningsprosjekter som er basert på utvalg, er å tilordne hver respondent et eget løpenummer. For å styrke respondentenes tillit til at de kan forbli anonyme, kan forskeren sette bort tilordningsprosessen til en uavhengig tredjepart. Denne metoden fungerer godt for enkeltstående undersøkelser. Dersom man gjennomfører en panelstudie med de samme respondentene over tid, blir håndteringen av løpenumre gradvis vanskeligere. Å koble data med relevante data fra andre kilder ville forutsette en åpenlys reversering av de tilordnede løpenumrene. Som

5 David L. Chaum: *Untraceable electronic mail, return addresses, and digital pseudonyms*. I: Communications of the ACM. Årg. 24 nr. 2, s. 84-90 (1981)

6 Kjent også på norsk gjennom forkortelsen PKI (Public Key Infrastructure)

7 David L. Chaum: *A New Paradigm for Individuals in the Information Age*. 1984 IEEE Symposium on Security and Privacy, s. 99-103, IEEE Computer Society Press, Washington (1984)

pseudonymer blir slike løpenumre rent illusoriske. Å bytte ut en reell identifikasjon av respondenten med et tilfeldig løpenummer gir bare tilfredsstillende sikkerhet hvis forskeren ikke skal tilføye nye opplysninger senere eller koble med andre kilder. Det er ikke en holdbar metode for et helseregister som skal tjene sammensatte formål over lengre tid.

Pålitelige digitale pseudonymer i et helseregister forutsetter bruk av avansert kryptografi. Et entydig identifikasjonsnummer, som ikke endres over tid for samme pasient, er nødvendig som input til algoritmen som genererer pseudonymet. I Norge er fødselsnummeret godt egnet til det formålet. Helseregisteret trenger ikke lagre fødselsnummeret, algoritmen sørger for at det samme pseudonymet blir tilordnet samme pasient hver gang nye opplysninger tilføyes til registeret.

Når man først har en pålitelig og entydig identifikator, kan pseudonymer genereres på to prinsipielt forskjellige måter. Den ene måten er å bruke en asymmetrisk hash-funksjon. Det innebærer at krypteringsalgoritmen genererer et resultat («hash-verdi») som er entydig for samme fødselsnummer, men uten at pseudonymet kan dekrypteres tilbake til samme input etterpå. Ettersom samme fødselsnummer alltid vil generere samme resultat, er det mulig å legge til flere opplysninger om samme pasient i samme helseregister. Det skal imidlertid ikke uten videre være mulig å koble data på individnivå mellom to forskjellige helseregistre.[8] Denne metoden sikrer høy grad av konfidensialitet, men er på den annen side lite fleksibel. Det vil være svært vanskelig å koble eller slå sammen to helseregistre, og det vil være vanskelig å spore opp og kontakte enkeltpasienter, for eksempel dersom en ny behandlingsmetode kan forbedre helsehjelpen til pasienter som har en bestemt sykdom.

Den andre metoden for å generere et pseudonym er nærmere beslektet med PKI-basert krypteringsteknologi, og er grunnleggende den samme som Chaum argumenterte for.[9] Den samme varige og entydige identifikatoren brukes som input. En krypteringsalgoritme, som bruker den offentlige nøkkelen i et nøkkelpar, genererer pseudonymet. Det samme fødselsnummeret, og den samme offentlige nøkkelen, gjør det mulig å tilføye nye data om samme pasient i et register. I tillegg vil en dekrypteringsalgoritme kunne reversere pseudonymet tilbake til det faktiske fødselsnummeret, ved å bruke den private nøkkelen av samme nøkkelpar som ble brukt til krypteringen. En uavhengig, tiltrodd pseudonymforvalter utfører krypteringen, og om ønsket også dekrypteringen.

8 Ettersom antallet mulige gyldige fødselsnumre i Norge er temmelig begrenset, vil en pseudonymforvalter i praksis kunne reversere denne typen pseudonymer ved å kjøre alle gyldige fødselsnumre gjennom algoritmen. Derfor er det nødvendig med en ekstern, tiltrodd pseudonymforvalter selv om man velger denne typen enveis krypteringsalgoritme.

9 se avsnitt 1.2 ovenfor

Helseregisteret vil aldri se den enkelte pasients reelle identifikator. Den tiltrodde tredjeparten, som genererer pseudonymet, kjenner bare koblingsinformasjonen uten å sitte med noen helseopplysninger om pasientene. En PKI-basert metode gir større fleksibilitet, men innebærer også at pseudonymene blir noe skjørere. Pasientens konfidensialitet blir i større grad avhengig av tillit til den uavhengige tredjeparten. Det vil være teknisk gjennomførbart å avdekke helseopplysninger om en identifisert pasient dersom både helseregisteret og pseudonymforvalteren bidrar til det.

De to eksisterende pseudonyme helseregistrene i Norge bruker en slags kombinasjon av de to metodene beskrevet ovenfor. Kommunikasjonen mellom de rapporteringspliktige enhetene og pseudonymforvalteren, og deretter mellom pseudonymforvalteren og helseregisteret, er basert på PKI. Selve pseudonymet som genereres er ureverserbare hash-verdier, som er generert med fødselsnummeret som input.[10] Likevel kan ikke de prinsipielt sett ureverserbare hash-verdiene fullt ut garantere mot uautorisert reversering av pseudonymene. På grunn av det relativt lave antallet mulige unike fødselsnumre, som det også er forholdsvis enkelt å generere fullstendig oversikt over, kan den som kjenner algoritmen sette sammen en fullstendig liste over de pseudonymer som svarer til hvert eksisterende eller potensielt eksisterende fødselsnummer. Av den grunn forutsetter sikkerheten ved pseudonyme helseregistre at pseudonymene byttes ut med ikke altfor lange mellomrom.

2 Støtte for digitale pseudonymer i lovgivningen

Vanligvis skjer utviklingen av teknologiske nyvinninger så raskt og brått at det gjerne etterlater et inntrykk av at lovgivningen blir liggende på etterskudd. Samfunnets verktøykasse for å beskytte verdier og fordele plikter og rettigheter tilpasses teknologiske endringer som allerede har funnet sted.

Innføringen av pseudonymer i norske helseregistre har imidlertid ikke vært noen etterskuddsvis tilpasning. Det første pseudonyme helseregisteret ble etablert i 2004. På det tidspunkt hadde deltakere i ulike lovgivningsprosesser allerede gått inn for slike pseudonymer i mer enn et tiår. Både teknologer og profesjonelle brukere av registrene forble skeptiske. Utviklingen av pseudonyme helseregistre har på ingen måte vært teknologistyrt i Norge, det ville være mer treffende å betegne utviklingen som lovgivningsstyrt.

10 I realiteten er det litt mer komplisert: Først hentes det såkalte «S-nummeret» for fødselsnummeret frem, det er et bindeledd som identifiserer samme person entydig også dersom han av en eller annen grunn har skiftet fødselsnummer. Deretter genereres pseudonymet fra «S-nummeret»

2.1 Et tidlig og avantgardistisk lovforslag

I Norge har man hatt ulike registre for spesifikke kategorier av sykdommer, som for eksempel Kreftregisteret, i flere tiår. Til å begynne med var registrene papirbaserte, og ble senere lagt om til elektronisk lagring og bearbeiding. De diagnosespesifikke registrene hadde vist seg nyttige over lang tid. Etter hvert fikk helsemyndighetene også et ønske om å etablere et generelt nasjonalt helseregister, som ikke skulle være avgrenset til bestemte sykdommer.

Selv om fordelene ved et generelt nasjonalt helseregister var overbevisende, var Stortinget svært bekymret for konsekvensene for pasientenes personvern. I 1989 ba de regjeringen utnevne et utvalg som skulle utrede tiltak og metoder for å kunne etablere et slikt register «uten å overkjøre den enkeltes personvern».[11]

Utvalget avga sin utredning i 1993.[12] Der foreslo de en ny lov som hjemlet et generelt nasjonalt helseregister. Lovutkastet var langt forut for sin tid. Det inneholdt forslag til bestemmelser om kryptografiske pseudonymer, generert og forvaltet av tiltrodde tredjeparter, i tillegg til omfattende bestemmelser som skulle sikre berettiget bruk av registeret, datakvalitet, pasientenes rett til innsyn med videre.

Imidlertid var verken helsemyndighetene eller de medisinske og helsefaglige forskningsmiljøene særlig begeistret for denne avantgardistisk måten å organisere det nye helseregisteret på. Ettersom de viktigste interessentene ikke støttet forslaget ble det satt på vent, og der forble det i omtrent åtte år.

I første omgang ble det verken etablert et fullt ut identifiserbart register (som var det helsemyndigheter og forskere ønsket) eller et pseudonymt register (forslaget som ble avvist). I stedet etablerte helsemyndighetene Norsk pasientregister[13] i 1997. Det ble opprinnelig etablert som et avidentifisert[14] register. Dette var gjennomførbart i tråd med den daværende personregisterloven,[15] og kunne iverksettes uten lovendring.

2.2 Personopplysningsrettslig spesiallov om helseregistre

Relativt kort tid etter at personopplysningsloven erstattet personregisterloven, ble det også vedtatt en ny spesiallov om behandling av helseopplysninger i hel-

11 Erik Boe: *Pseudo-identities in Health Registers: Information technology as a vehicle for privacy protection*. I: The International Privacy Bulletin. Årg. 2 nr. 3, s. 8-13 (1994)
12 NOU 1993:22 *Pseudonyme helseregistre*
13 se avsnitt 3.3 nedenfor
14 se avsnitt 2.3 nedenfor
15 lov 9. juni 1978 nr. 48, *om personregistre m.m.* (opphevet)

setjenesten og helseforvaltningen.[16] Hovedregelen for berettiget behandling av helseopplysninger er et krav om å innhente pasientenes samtykke. Loven åpner imidlertid også for at det i visse situasjoner kan være behov for å behandle opplysninger uten samtykke. Blant de forhold som kan berettige behandling av opplysninger uten samtykke er helseregistre der fullstendig dekning er nødvendig for å ivareta registerets formål.

2.3 Fire forskjellige nivåer av pasientidentifisering i helseregistre

Hovedbestemmelsen for sentrale helseregistre, som samler opplysninger fra ulike behandlingsinstitusjoner, er helseregisterlovens § 8. Utgangsposisjonen er at sentrale helseregistre ikke er tillatt, med mindre de har hjemmel i helseregisterloven eller annen lov. Resten av § 8 angir mulighetene og betingelsene for å etablere helseregistre, dersom de har adekvat hjemmel. Formålet med et sentralt register skal være «ivaretakelse av oppgaver etter [ulike nærmere spesifiserte lover]». Ivaretakelse av oppgavene omfatter også «overordnet styring og planlegging av tjenestene, kvalitetsutvikling, forskning og statistikk». Kravet til samtykke kan fravikes dersom forskrift om det konkrete, sentrale registeret bestemmes at opplysningene bare kan behandles i pseudonymisert eller avidentifisert form.

Dermed innfører § 8 en interessant klassifisering av helseregistre i ulike nivåer av pasientidentifisering. Hvert nivå gir en egen kombinasjon av handlingsrom og plikter for registermyndigheten, og en egen grad av identifiserbarhet for pasienten. Alle sentrale helseregistre må innordnes under et av disse nivåene. Valget av identifiseringsnivå er i seg selv en viktig del av balanseringen mellom samfunnsinteresser og personverninteresser ved etableringen av det enkelte register.

Personopplysninger			Ikke personopplysning
Personentydige opplysningstyper		Ikke personentydige opplysningstyper	
Personidentifiserbar	Pseudonym	Avidentifisert	Anonym

Figur 1: Skisse over nivåene av pasientidentifisering[17]

16 lov 18. mai 2001 nr. 24, *om helseregistre og behandling av helseopplysninger (helseregisterloven)*

17 Denne skissen er lånt fra Åsa L'Abée-Lund: *Pseudonymisering av personopplysninger i sentrale helseregistre*. Masteravhandling i forvaltningsinformatikk, Universitetet i Oslo (2006), s. 28

Den nederste raden i tabellen viser de fire forskjellige nivåene av pasientidentifisering. Rekkefølgen, fra venstre til høyre, gjenspeiler rekkefølgen fra større til mindre belastning på pasientenes personopplysningsvern.

Den midterste raden i tabellen viser hvor hovedskillet går mellom de opplysningene som refererer til entydige pasienter og de som ikke gjør det. Fullt identifiserbare pasienter og pseudonyme pasienter har samme statistiske målenivå.

Den øverste raden viser at det bare er tre av de fire identifiseringsnivåene som strengt tatt hører inn under definisjonen av personopplysninger, og som derfor er omfattet av begrensningene i helseregisterlovens § 8.

Hovedregelen er at fullt identifiserbare helseregistre bare kan behandle opplysninger om personer som samtykker til det. De eneste unntakene er et beskjedent antall helseregistre som er konkret anført i § 8 tredje ledd. Det er for tiden nøyaktig ni fullt identifiserbare sentrale helseregistre i Norge der pasientens samtykke ikke er påkrevd.[18] For hvert nye, sentrale helseregister som skal ha full entydig identifikasjon av pasienten, uten å innhente samtykke, må Stortinget vedta en lovendring som spesifikt tilføyer dette registeret med navns nevnelse i helseregisterlovens § 8. Dette er etter mitt syn en vakker konstruksjon; det sikrer en åpen, bred og demokratisk prosess forut for etableringen av de mest inngripende helseregistrene.

Ved å bruke pseudonymer i stedet for fullstendig identifikasjon, kan et nytt helseregister etableres ved forskrift. Et pseudonymt register i tråd med rammene i helseregisterloven krever ikke lovendring. Det er heller ikke påkrevd at registeret baseres på samtykke, dersom det er nødvendig å samle fullstendige opplysninger om en populasjon. Pseudonyme helseregistre, som et selvstendig alternativ for balansering av registres behov og pasienters personopplysningsvern fikk altså sin plass i lovverket i 2001, åtte år etter at det først ble foreslått.

Et avidentifisert og et pseudonymt helseregister er i prinsippet likeverdige som grunnlag for å etablere sentrale helseregistre etter helseregisterlovens § 8. Helsemyndighetene kan etablere et avidentifisert register ved forskrift. Et avidentifisert register innebærer at alle entydig identifiserende opplysninger er fjernet. Avidentifiseringens fordel fremfor pseudonymer er at det avidentifiserte registeret er teknisk enklere og mindre kostbart i drift. Den klart største ulempen ved avidentifisering er at opplysningene ikke er personentydige i streng forstand. Hvis et sykehus gjennomfører samme kirurgiske operasjon for eksempel fire ganger, kan ikke et avidentifisert register skille mellom en situasjon der samme pasient er operert fire ganger og en situasjon der fire forskjellige pasienter er operert én gang hver.

18 Da helseregisterloven trådte i kraft 1. januar 2002 var det seks slike spesifiserte registre

Pseudonyme og avidentifiserte registre deler samme grad av risiko for urettmessig *re*-identifisering gjennom systematisk analyse av de lagrede opplysningene.[19] Sannsynligheten for å avdekke identiteten til en entydig person øker med variablenes antall og detaljnivå. Å hanskes med faren for re-identifisering forutsetter for det første at den ansvarlige vurderer nøye og kritisk hvilke opplysninger det egentlig er behov for å lagre. Dernest må man være oppmerksom på at behovet for snever tilgangskontroll og andre konvensjonelle informasjonssikkerhetstiltak fremdeles er tilstede selv om registeret er pseudonymt eller avidentifisert.

I det fjerde nivået av pasientidentifisering, anonyme registre, skal alle opplysninger som overhodet gjør det mulig å skille ut individuelle pasienter fjernes. I tillegg til å fjerne konkrete identifikatorer, må registeret også fjerne, eller omklassifisere til mer generelle kategorier, alle opplysninger som kan innebære risiko for re-identifisering gjennom systematisk analyse. Et anonymt register tar opplysningenes konkrete granularitet med i betraktningen.[20] Å anonymisere data innebærer ofte en målrettet handling for å svekke presisjonsnivået.

Reelt anonymiserte opplysninger kan gjerne publiseres, og krever ingen omfattende beskyttelsestiltak. Ulempen ved anonyme opplysninger, som i de fleste tilfeller gjør dem fullstendig uegnet som pasientidentifiseringsnivå i et varig helseregister, er at det praktisk talt er umulig å tilføye nye opplysninger til registeret på en meningsfull måte.

2.4 Fagmiljøenes operative ansvar, og en demokratisk sikkerhetsventil

Helseregisterloven åpner altså for fire ulike prinsipper for pasientidentifikasjon i helseregistre. Alle de fire nivåene av pasientidentifisering finnes i eksisterende helseregistre. Alle fungerer i praksis, og fyller sin hensikt. De fire nominale nivåene utgjør i seg selv et relativt objektivt verktøy for en saklig og opplyst debatt om personvernavveiningene knyttet til et planlagt eller eksisterende re-

19 Bradley Malin: *Betrayed by My Shadow: Learning Data Identity via Trail Matching*. Journal of Privacy Technology (elektronisk tidsskrift). Paper number 20050609001. Pittsburg, PA (2005) http://www.jopt.org/publications/20050609001_malin.pdf (lesedato: 16. oktober 2009)

20 Kravene til anonymisering ligger ikke helt fast, men ofte brukes som tommelfingerregel at en opplysning er anonym dersom den ikke kan tilbakeføres til færre enn fire individer. Dette er for eksempel lagt til grunn i departementets publiserte kommentarer til *SYSVAK-forskriften* (20. juni 2003 nr. 739) § 3-1 (bestemmelse om at sammenstillinger av opplysninger fra det personidentifiserbare registeret SYSVAK med visse andre navngitte registre er tillatt hvis det skjer i anonymisert form). I kommentaren heter det: «Hvorvidt tabelldataene eller statistikken er tilstrekkelig anonymisert, må vurderes i hvert enkelt tilfelle. Ved publisering av tabeller på lokalt og regionalt nivå har det i praksis vært lagt til grunn 4 eller 5 enheter.»

gister. Man vet hva de alternative identifiseringsnivåene er, og man vet hvordan de virker. For hvert av nivåene er det forholdsvis klart hvordan de påvirker balansen mellom pasientens personvern versus presisjonsnivået i opplysninger til helsemyndighetenes beslutningsstøtte og forskning.

Som databehandlingsansvarlige har vedkommende helsemyndighet eller forskningsmiljø det formelle og praktiske ansvar for alle aspekter ved de enkelte helseregistre. Imidlertid utgjør de rigide kravene som stilles for å kunne etablere et fullt personidentifiserbart register (som ikke baseres på informert samtykke) en omhyggelig plassert demokratisk sikkerhetsventil. For hvert slikt register som skal etableres må Stortinget vedta en konkret endring i helseregisterlovens § 8. Fagmiljøene behøver ikke, og kan heller ikke, beslutte på egen hånd å etablere registre som er så inngripende for personopplysningsvernet. Selv om prosessen for å hjemle et register i formell lov kan være kronglete og tidkrevende, sikrer det også en høy grad av demokratisk deltakelse i arbeidet med å balansere personverninteresser mot det enkelte personidentifiserbare helseregisterets velbegrunnete nytteverdi.

3 Fire konkrete forslag – som ble til to pseudonyme helseregistre

Så langt har Helse- og omsorgsdepartementet vurdert og behandlet forslag om etablering av pseudonyme helseregistre i fire ulike tilfeller. I to av disse tilfellene ble det foreslåtte registeret etablert med pseudonymer som pasientidentifiseringsnivå. I de to andre tilfellene der forslag om pseudonymer har vært behandlet, ble det ene registeret «forfremmet» til fullt personidentifiserbart, mens det andre ble «degradert» til et avidentifisert register.

3.1 Reseptregisteret

Norges første nasjonale, pseudonyme helseregister er *Reseptregisteret*. Helse- og omsorgsdepartementet ga forskrift om dette registeret i 2003,[21] det ble etablert i begynnelsen av 2004.

Før reseptregisteret var medikamentstatistikker basert på salgstall rapportert fra grossistene. Datagrunnlaget var utvilsomt utilstrekkelig som kilde til kunnskap om bruken av medikamenter. Flere instanser hadde behov for statistikk basert på forskrivning og på hvilke medisiner den enkelte pasient faktisk henter på apoteket. Formålet med registeret er kun å skaffe dette datagrunnlaget, det skal hverken brukes til å overvåke enkeltpasienters fangst på apoteket eller til å kontrollere legers forskrivningspraksis. Pseudonymer er tilstrekkelig

21 Forskrift 17. oktober 2003 nr. 1246

identifiseringsnivå for å oppnå registerets formål, samtidig som det gir høy grad av sikkerhet mot at registeret kan brukes til andre formål i strid med pasientenes og legenes personverninteresser.

Alle apotekene rapporterer reseptopplysningene elektronisk hver måned. Et sentralt dataoppsamlingspunkt overfører dataene til en tiltrodd tredjepart. Pseudonymforvalteren for reseptregisteret er Statistisk sentralbyrå. De overfører pseudonymene til Folkehelseinstituttet, som er ansvarlig for registeret. Både pasientens fødselsnummer og legens helsepersonellnummer blir erstattet med pseudonymer. Apotekene er fullt identifisert på virksomhetsnivå; apotekkonsesjonsnummeret er ikke pseudonymisert.[22]

Innføringen av reseptregisteret var i det store og hele en «stille reform». De endringene det medførte har praktisk talt vært usynlige for pasientene. De får fremdeles utlevert en resept som de tar med seg til apoteket på samme måte som før. De blir ikke bedt om å samtykke til at opplysningene rapporteres. Reseptregisterets eksistens er ikke på noen måte hemmelig, men det er heller ikke noe som angår pasientene i særlig grad. Antakelig er det bare de som har en nokså detaljert innsikt i helsepolitikk og tilhørende personvernspørsmål som kjenner til de pseudonyme registeropplysningene.

3.2 Pleie- og omsorgsbehov, IPLOS

Det andre pseudonyme helseregisteret heter *IPLOS*, som er et akronym for individbasert pleie- og omsorgsstatistikk. Helse- og omsorgsdepartementet ga forskrift om dette registeret i 2006.[23] Den første obligatoriske rapportterminen var februar 2007, med innrapportering av opplysninger fra alle landets kommuner. Helsedirektoratet er ansvarlig for registeret. Skatteetaten ble valgt som tiltrodd pseudonymforvalter, noe som illustrerer poenget om at det viktigste kriteriet en pseudonymforvalter må innfri er institusjonell uavhengighet.

I motsetning til reseptregisteret, har IPLOS slett ikke vært noen stille reform. Opplysningene om individers pleiebehov kunne ikke hentes ut fra noen allerede eksisterende informasjonsprosesser. Selv om pasientene bør kunne kan ha tillit til at de pseudonyme opplysningene er godt beskyttet i det sentrale registeret, er det ikke like opplagt at konfidensialiteten ivaretas godt nok når et nytt skjema med nye og til dels intime spørsmål skal besvares lokalt. Noen har jobben med å taste svarene inn i en lokal database, med full identifikasjon, før de sendes videre til det sentrale, pseudonyme registeret. Det største problemet

22 Hanne Strøm: *Reseptbasert legemiddelregister.* I: Norsk Farmaceutisk Tidsskrift. Årg. 112 nr. 1, s. 7-9 (2004)

23 Forskrift 17. februar 2006 nr. 204

er i dette tilfellet ikke hvorvidt pseudonymet gir tilstrekkelig konfidensialitetsvern. Mange pasienter ble både provosert og følte seg støtt over de spørsmålene i skjemaet som de enten synes var for intime, eller som de ikke kunne være enige i at var relevante for deres egen situasjon. Skjemaene ble endret som et resultat av klager på en del av spørsmålene, for eksempel spørsmål om pasienten trengte hjelp etter toalettbesøk eller under menstruasjon.

Pseudonymer er et virkemiddel som bare kan avhjelpe noen av de personvernproblemene som oppstår etter at pasienten er ferdig med sitt bidrag til at opplysningene produseres. Helseregistre håndterer i de fleste tilfeller opplysninger som rapporteres inn etterskuddsvis, og løsrevet fra pasientens deltakelse. For registre som ikke er basert på samtykke vil pasienten knapt merke at opplysningene eksisterer. I en del tilfeller vil derfor grensene for hva slags helseregistre det er mulig å opprette ikke handle om hvor godt man vil eller kan sikre selve registeret, men om hvor inngripende pasientene opplever prosessen med å produsere eller samle inn opplysningene.

3.3 Norsk pasientregister

Norsk pasientregister, med akronymet *NPR*, er et helseregister med informasjon om alle sykehusinnleggelser og polikliniske konsultasjoner. Data om hver pasient samles inn fra alle landets sykehus. Dette registeret er et interessant innslag i det norske personopplysningsvernets historie. NPR er realiseringen av det «generelle, nasjonale helseregisteret» som var bakgrunnen for Boeutvalget, som ble oppnevnt i 1989 og foreslo pseudonyme registre som løsning i sin rapport fra 1993.

Etter at forslaget om pseudonyme helseregistre ble lagt på vent, ble ønsket om et generelt helseregister gjenopplivet med forslaget om å etablere NPR som et avidentifisert register. Det ble etablert i mars 1997. NPR mottar rapporter om medisinske behandlinger fra alle sykehusenes pasientadministrative systemer. Alder, kjønn, bosted, sykehus og sykehusavdeling, diagnose, type behandlingsprosedyre og datoer for innleggelse og utskriving inngikk i det avidentifiserte registeret.[24] Navn og fødselsnummer ble ikke tatt med.

NPR viste seg å være et nyttig og verdifullt register, dataene er etterspurt både til forskning og administrative formål. Likevel var begrensningene som lå i at registeret var avidentifisert åpenbare. Dataene var ikke personentydige,

24 Inger Johanne Bakken, Kari Nyland, Vidar Halsteinli, Unn Huse Kvam og Finn Egil Skjeldestad: *Norsk pasientregister. Administrativ database med mange forskningsmuligheter.* I: Norsk epidemiologi. Årg. 14 nr. 1, s. 65-69 (2004)

man kunne ikke vite sikkert om flere lignende tilfeller gjaldt samme pasient eller forskjellige pasienter.

Etter noen år med etterspurte data, som likevel hadde noe begrenset nytteverdi, begynte helsemyndigheter og fagmiljøer å arbeide politisk for å styrke registerets målenivå, ved å gjøre det personidentifiserbart. Motstandere av en slik endring argumenterte med at det ville være tilstrekkelig for formålet å gjøre NPR til et pseudonymt register. Helsemyndighetene og de medisinske forskningsmiljøene argumenterte med at et pseudonymt register ikke kunne garantere tilstrekkelig datakvalitet. Etter en opphetet debatt ble forslaget om et personidentifisert NPR fremmet for Stortinget, som vedtok å føye Norsk pasientregister til listen over sentrale personidentifiserte helseregistre i helseregisterlovens § 8 tredje ledd. Lovendringen ble vedtatt 1. februar 2007. Forskriften som regulerer «nye» NPR, som fullt personidentifisert helseregister, ble gitt i desember same år.[25]

3.4 Abortregisteret

Det hittil siste eksemplet på at Helse- og omsorgsdepartementet har realitetsbehandlet et forslag om å gjøre et register pseudonymt er Abortregisteret. Et forslag om å etablere Abortregisteret som pseudonymt register var ute på høring, med svarfrist 13. januar 2006. Svært mange av høringsinstansene var skeptiske til et register med et så sensitivt innhold som en fullstendig oversikt over aborter ville være.

Forslaget ble møtt med uvilje fra ulike hold. Mange av høringssvarene pekte på den spesielle belastningen det er for mange kvinner å bestemme seg for å gjennomføre en abort. Selv om kvinner har rett til selvbestemt abort vil valget for noen være forbundet med en fare for sosiale sanksjoner eller fordømmelse fra nærstående eller fra sin religiøse tilknytning. Med dette som bakgrunn argumenterte blant annet Datatilsynet for at kjennskapen til et abortregister i noen tilfeller kunne få innvirkning på enkeltes beslutning om å ta abort eller ikke. Dermed kunne situasjonen bli at et helseregister selv påvirket, og ikke bare reflekterte, helsetjenestens virksomhet. Regjeringen besluttet 21. juni 2007 at Abortregisteret skulle være et avidentifisert, og ikke pseudonymt, register.

Forslaget og debatten om Abortregisteret avdekket en interessant begrensning i tilliten til pseudonyme registre. Pseudonymets konfidensialitet er basert på en tillit som gjelder samfunnet slik vi kjenner det i dag. Selv om reversering av pseudonymer er tungvint, og vil kreve samarbeid med den tiltrodde pseu-

25 Forskrift 7. desember 2007 nr. 1389

donymforvalteren, må man likevel ta på alvor mulighetene for at pseudonymene kan reverseres i en fremtid der holdningene til personopplysningsvernet er ukjent.

4 Konklusjoner

4.1 Pseudonymer fungerer

Digitale pseudonymer er et tilgjengelig og rettslig regulert virkemiddel for å beskytte personentydige helseopplysninger som samles inn og lagres i lang tid i norske helseregistre. Siden 2001 har det vært tillatt som ett av fire ulike alternative identifiseringsnivåer. Ved bruk av avanserte teknologiske og forvaltningsmessige prosedyrer gir det anledning til å kombinere høy grad av konfidensialitet med høy faglig nytteverdi. Det er likevel bare etablert to pseudonyme helseregistre hittil. Antallet er betydelig høyere både for fullt personidentifiserbare og for avidentifiserte registre.

En case-studie av Reseptregisteret viste at pseudonyme registre i det store og hele fungerer etter hensikten.[26] Verken den tiltrodde pseudonymforvalteren eller den ansvarlige for registeret – eller noen annen for den saks skyld – har tilgang samtidig til både fødselsnummer og ukrypterte helseopplysninger knyttet til det enkelte individ. Til å begynne med var det visse problemer med datakvaliteten, men etter hvert gikk feilprosenten ned mot omtrent samme nivå som man har i personidentifiserbare registre.

4.2 Pseudonymer er likevel fremdeles kontroversielle

Denne korte gjennomgangen av forslagene og debattene om pseudonyme helseregistre i Norge synliggjør noen hovedkategorier av argumenter for og mot digitale pseudonymer.

Det primære argumentet for pseudonyme helseregistre er den reduserte risikoen for at opplysninger om en identifisert pasient røpes til personer som ikke har behov for opplysningene, eller til personer som trenger opplysningene, men ikke behøver å kjenne pasientens reelle identitet. Pseudonymene styrker personopplysningsvernet, samtidig som opplysningenes statistiske nøyaktighet og målenivå opprettholdes.

Motargumentene er mer sammensatte: Økte kostnader på grunn av teknisk kompleksitet og den eksterne pseudonymforvaltningsprosessen, faren for re-

26 Åsa L'Abée-Lund: *Pseudonymisering av personopplysninger i sentrale helseregistre*. Masteravhandling i forvaltningsinformatikk, Universitetet i Oslo (2006)

identifisering ved systematisk analyse av registerets øvrige opplysninger, og faren for en uforutsett forverring av personopplysningsvernets status i samfunnet i fremtiden. Og til sist, et av de argumentene som oftest brukes mot pseudonyme helseregistre, er datakvalitetsproblemet. Den som er ansvarlig for registeret vil ha mer begrensede muligheter for å avdekke og korrigere feil på egen hånd. Problemene kan imidlertid håndteres, først og fremst gjennom forbedring av kvaliteten på det som rapporteres, og kanskje til en viss grad ved å samarbeide med pseudonymforvalteren om strukturerte «registervask»-prosedyrer.

Når man ser på de argumentene som brukes, for eller mot pseudonyme helseregistre, kan støynivået og graden av polarisering virke noe overdrevet. Pseudonyme helseregistre er ganske enkelt en mellomposisjon i valget av pasientidentifiseringsnivå. Å bevege seg ett skritt til venstre eller ett skritt til høyre (med referanse til figur 1 ovenfor), innebærer en nyanseforskjell i hvordan man vurderer balansen mellom registerets nytteverdi og ulempene for personopplysningsvernet. Valget av et høyere eller lavere pasientidentifiseringsnivå fjerner verken de gevinstene eller de problemene som et pseudonymt register skaper fullt og helt. Et forslag om å gjøre et konkret helseregister pseudonymt kan forvente motstand fra begge sider; noen vil mene at personentydigheten truer personvernet selv om identifikatoren erstattes av et pseudonym, andre vil mene at behovet for å involvere en ekstern pseudonymforvalter, blant annet ved sammenstilling av data fra andre kilder, legger for store begrensninger på registerets nytteverdi.

Etter min oppfatning er det faktum at det så langt bare er etablert to pseudonyme helseregistre etter at helseregisterloven ble vedtatt, mens Stortinget har akseptert tre nye fullt personidentifiserbare register i samme periode, dessverre et tegn på at tilhengerne av pseudonyme helseregistre synes å kjempe en tapt kamp. Likevel synes jeg helseregisterlovens innretning med egne regler for hvert av identifiseringsnivåene er en god konstruksjon. Denne innretningen sikrer en åpen demokratisk prosess om de mest inngripende registrene, og sørger for å påkalle ulike interessenters oppmerksomhet slik at ulike syn kommer til uttrykk.

DATATILSYNETS VIRKEMIDDELBRUK[1]

Tommy Tranvik

Innledning

Reglene i lover og forskrifter implementerer seg ikke selv: individer eller organisasjoner følger ikke alltid opp reguleringenes ånd og bokstav bare fordi lovverket krever det av dem. Derfor benytter staten ulike implementeringsmekanismer som skal sørge for at lover overholdes, forskrifter praktiseres og regulatoriske målsettinger realiseres. Én av disse implementeringsmekanismene er tilsynsorganer, og effekten av rettslige reguleringer – hvorvidt plikt- og rettighetssubjekters atferd endres slik at regulatoriske formål oppnås – antas i stor grad å bero på hvilke virkemidler tilsynsorganene er utstyrt med og hvordan de benyttes.[2]

Denne artikkelen drøfter Datatilsynets virkemidler og virkemiddelbruk.[3] Spørsmålene som diskuteres er (a) hvilke virkemidler har Datatilsynet til rådighet, (b) hvordan brukes virkemidlene for å påvirke kommunenes praktisering av personopplysningslovens og personopplysningsforskriftens bestemmelser om informasjonssikkerhet[4] og (c) hvilke effekter (om noen) har virkemiddelbruken på graden av kommunal regeloverholdelse?

Det rettslige utgangspunktet for artikkelen – personopplysningslovens og forskriftens bestemmelser om sikring av personopplysninger – er valgt fordi

---

1 Denne artikkelen springer ut av forskningsprosjektet *Legal Information Security Regulations: An Instrumental Perspective* utført ved Avdeling for Forvaltningsinformatikk, Universitetet i Oslo. Prosjektet er finansiert av Norges Forskningsråd over programmet *IKT, sikkerhet og sårbarhet*.

2 Statlig styring ved hjelp av rettsregler og tilsynsorganer defineres på følgende måte: «(…) the promulgation of an authoritative set of rules, accompanied by some mechanism, typically a public agency, for monitoring and promoting compliance with these rules» (Baldwin et al. 1998: 3).

3 Datatilsynet ble etablert i 1979 (og var operativt fra 1. januar 1980). Fra og med 1. januar 2001, har personopplysningsloven og forskriften vært de viktigste rettslige reguleringene som Datatilsynet forvalter.

4 Personopplysningsloven (med forskrift) gjelder for alle som behandler personopplysninger helt eller delvis med elektroniske hjelpemidler, eller hvis det opprettes manuelle personregistre. Personopplysninger defineres som opplysninger som kan knyttes til fysiske personer: alt fra kontaktinformasjon – navn, adresse og telefonnummer – via fødselsnummer og informasjon om fritidssysler, livssyn eller sosiale forhold, til konto- og helseopplysninger (jf. personopplysningsloven § 2).

håndhevingen av bestemmelsene er høyt prioritert i Datatilsynet. Samtidig representerer disse reglene en særlig krevende og komplisert del av personvernlovgivningen.[5] Kombinasjonen av høy prioritet og kompliserte regler gjør at informasjonssikringsområdet kan sies å være en prøvestein for Datatilsynets generelle virkemiddelbruk: Hvordan virkemiddelbruken fungerer på dette området kan gi et visst innblikk i hvordan den fungerer i forhold til andre deler av personvernlovgivningen.

Kommunesektoren er valgt som studieobjekt for Datatilsynets virkemiddelbruk fordi kommunene behandler store mengder personopplysninger, spesielt innenfor tunge velferdsområder som helse, pleie/omsorg og skole. Hvordan kommunene sikrer disse opplysningene kan derfor ha stor betydning både for innbyggernes personvern og for tilliten til det lokale administrative og tjenesteproduserende apparatet. Samtidig fører kommunenes rolle som velferdsstatens hovedtilbydere av tjenester til at Datatilsynet er spesielt opptatt av hvordan reglene om informasjonssikkerhet (og de øvrige delene av personvernlovverket) praktiseres i denne delen av offentlig forvaltning.

Nedenfor drøftes først Datatilsynets organisering og hvilke virkemidler Datatilsynet er utrustet med. Deretter drøftes bruken av tilsynsorganets to hovedvirkemidler: (1) kontroller og sanksjoner og (2) informering og veiledning. Til slutt gis en kort og tentativ analyse av hvilke effekter bruken av disse virkemidlene kan sies å ha på kommunenes overholdelse av bestemmelsene om informasjonssikkerhet.[6]

---

5 Se for eksempel Tranvik 2010a og Schartum 2005.

6 Datainnsamlingen som denne artikkelen bygger på ble gjennomført i 2007 og 2008. Hos Datatilsynet ble ledere og ansatte i alle avdelinger intervjuet, men med spesielt vekt på Tilsyns- og sikkerhetsavdelingen. Kontrollrapportene for samtlige stedlige kontroller i kommunesektoren, gjennomført i perioden 1. januar 2001 til 31. desember 2008, ble gjennomgått (her dreier det seg om 85 kontroller). Andre dokumenter – Datatilsynets årsmeldinger, interne strategier og policydokumenter, organisasjonsutredninger, informasjons- og veiledningsmateriale, lov- og forskriftskommentarer, høringsuttalelser, kampanje- og egenpresentasjonsmateriell, osv. – inngår også i datagrunnlaget. Flere kortere hospiteringsopphold – hvor Datatilsynet stilte kontorfasiliteter til rådighet – ble gjennomført som en del av datainnsamlingen. Data ble også innhentet fra 19 kommuner på østlandsområdet. To av kommunene kan defineres som mellomstore (begge hadde ca. 17 500 innbyggere), mens resten er store kommuner (mer enn 20 000 innbyggere). Kommunene fordeler seg på seks fylker: Oppland, Hedmark, Akershus, Buskerud, Vestfold og Østfold. Hensikten med denne delen av datainnsamlingen var bl.a. å kartlegge kommunenes overholdelse av personopplysningslovens og forskriftens bestemmelser om informasjonssikkerhet. I kommunene ble de operativt ansvarlige for informasjonssikringsarbeidet (sikkerhetsledere) og IT-sjefer intervjuet. I noen tilfeller ble rådmenn/assisterende rådmenn og kommunale personvernombud (der hvor det fantes) intervjuet. I tillegg ble kommunale plandokumenter – skriftlig materiale som beskrev hva kommunene hadde gjort for å ivareta regelverket – innhentet og analysert. Til slutt ble representanter for andre relevante institusjoner og organisasjoner intervjuet:

Datatilsynets organisering

Datatilsynet et lite tilsynsorgan. I 2008 forvaltet Datatilsynet 35 årsverk og et budsjett på litt i overkant av 26 millioner kroner.[7] De 35 årsverkene fordeler seg på fire avdelinger: Juridisk avdeling, Tilsyns- og sikkerhetsavdelingen, Informasjonsavdelingen og Administrasjonsavdelingen.[8] I motsetning til en del andre tilsynsorganer, har ikke Datatilsynet et regionalt organisatorisk apparat. Alle ansatte har derfor sitt arbeidssted ved Datatilsynets lokaler i Oslo sentrum.[9]

Administrativt er tilsynsorganet underlagt Fornyings- og administrasjonsdepartementet (FAD), men Datatilsynet har likevel stor grad av uavhengighet.[10] For det første ved at det er pålagt å utøve rollen som nasjonalt ombud på personvernområdet, det vil si å tale personvernets sak når personvernhensyn kolliderer med andre viktige samfunnshensyn.[11] For det andre ved at Datatilsynet kan gi uttrykk for synspunkter som går på tvers av de som forfektes i FAD. Dernest ved at klager på vedtak fattet av Datatilsynet ikke behandles i FAD, men av en egen klagenemnd – Personvernnemnda.[12] Og til slutt ved at FAD ikke har anledning til å påvirke hvordan Datatilsynet tolker reglene i personopplysningsloven og forskriften.[13]

Fornyings- og Administrasjonsdepartementet, Kommunenes Sentralforbund, Norsk Senter for Informasjonssikring, Personvernnemnda, Koordineringsutvalget for Forebyggende Informasjonssikkerhet, Foreningen for Kommunal Informasjonssikkerhet og IT-bransjen. Til sammen ble 62 intervjuer gjennomført (en rekke uformelle samtaler med kommunalt ansatte og ansatte i Datatilsynet inngår også i datamaterialet).

7 Se *Datatilsynets årsmelding for 2008*, s. 7.

8 Datatilsynet har tradisjonelt hatt en smal faglig sammensetning: de fleste ansatte (med unntak merkantilt personale) har vært jurister eller teknologer. I de senere årene er den faglige sammensetningen utvidet noe ved at det er rekruttert medarbeidere med samfunnsvitenskapelig og kommunikasjonsfaglig bakgrunn.

9 I NOU 2009: 1, *Individ og integritet. Personvern i det digitale samfunnet*, foreslås bl.a. opprettelse av regionale datatilsynsorganer (se kapittel 18). Det er uklart hvorvidt disse forslagene har støtte i Datatilsynet og hos overordnet departement.

10 Personopplysningsloven ligger inn under Justisdepartementets ansvarsområde, mens FAD forvalter personopplysningsforskriften.

11 Se personopplysningsloven § 42. Når Datatilsynet opptrer i rollen som nasjonalt personvernombud, er den årlige *Personvernrapporten* Datatilsynets viktigste publikasjon. Rapporten er ment å motivere virksomheter og individer til å tilegne seg kunnskap om personvernspørsmål.

12 Medlemmene i Personvernnemnda er dels utnevnt av regjeringen og dels av Stortinget (se personopplysningsloven § 43 og www.personvernnemnda.no).

13 Det er i særlig grad Datatilsynets direktør som har i oppgave å ivareta uavhengigheten, både i forhold til overordnet departement og overfor andre aktører i offentlig og privat sektor.

Datatilsynets virkemidler

Datatilsynet er utstyrt med en relativt omfattende kontroll- og sanksjonsmyndighet. Det kan for eksempel kreve tilgang til (a) all intern dokumentasjon knyttet til kommunenes (eller andre virksomheters) informasjonssikkerhetsarbeidet, (b) alle lokaliteter og teknologisystemer hos kommunene, og (c) be om bistand fra de ansatte ved gjennomføringen av kontroller.[14] Selv om Datatilsynet ikke kan stenge hele eller deler av virksomheten til brudd på informasjonssikkerhetsbestemmelsene er rettet,[15] kan Datatilsynet påpeke mangler i forhold til regelverket og fatte vedtak som pålegger kommunene å rette manglene. I tillegg kan Datatilsynet ilegge gebyrer og bøter (overtredelsesgebyr og tvangsmulkt) for alvorlige regelbrudd eller for manglende oppfølging av pålegg[16] (særlig alvorlige forhold kan politianmeldes[17]). Samtidig synes viljen til å anvende kontroll- og sanksjonsmyndigheten å være til stede. Ledere og ansatte i Datatilsynet mener at tilsynsorganer som ikke utfører kontroller – og som ikke reagerer på regelbrudd med sanksjoner – ikke gjør jobben sin.[18] Det kan derfor se ut som at oppdagelse og korrigering av regelbrudd spiller en viktig rolle i håndhevingsarbeid.[19]

Datatilsynets ombudsrolle på personvernområdet betyr imidlertid at hyppig bruk av tøffe sanksjoner (overtredelsesgebyr eller tvangsmulkt) ikke er uproblematisk: Datatilsynet kan da risikere å bli oppfattet som en «stivbeint

14 Se personopplysningsloven § 44. I § 45 presiseres det at ansatte i Datatilsynet har taushetsplikt for opplysninger som omfatter informasjonssikkerhetstiltak.

15 Men hvis konsesjoner for behandling av personopplysninger ikke fornyes, vil dette trolig innebære at hele eller deler av den aktiviteten som konsesjonen gjelder stopper opp.

16 Se personopplysningsloven §§ 46 og 47. Tvangsmulkt kan ilegges hvis tilsynsobjekter ikke etterkommer Datatilsynets pålegg om å rette feil eller mangler i forhold til regelverket, mens overtredelsesgebyr kan ilegges for feil eller mangler som oppdages ved stedlige eller brevlige kontroller.

17 Se personopplysningsloven § 48.

18 Internt i Datatilsynet har det vært en debatt om hvor omfattende kontrollvirksomheten trenger å være. Debatten har i særlig grad handlet om to forhold. For det første om Datatilsynet skal opprettholde eller øke antallet kontrollbesøk fra dagens nivå, eller om det bør brukes flere ressurser på informering, veiledning og rådgivning overfor de sektorene/bransjene som det føres kontroll med. For det andre om ansatte fra andre avdelinger enn Tilsyns- og sikkerhetsavdelingen bør delta i kontrollvirksomheten. Den siste debatten er løst ved at det nå settes sammen tverrfaglige tilsynsteam, mens den første debatten peker på ulike oppfatninger av hvordan kontrollvirksomheten bør integreres i den øvrige virkemiddelbruken.

19 Den økte betydningen av kontroller kommer bl.a. til uttrykk ved at Datatilsynet samordner deler av kontrollvirksomheten med andre tilsynsorganer (spesielt Helsetilsynet). I tillegg har Datatilsynet og FAD diskutert muligheten for å få til et prøveprosjekt med fylkesmennene om samordning av tilsyn.

regelrytter» eller en «nidkjær refser og straffer» av regelovertramp.[20] Et viktig spørsmål for Datatilsynet er derfor om bruken av sanksjonsvirkemidler bidrar til at tilsynsorganet nyter tillit, troverdighet og «goodwill» i rollen som «nasjonal fanebærer for personvernsaken»? Det betyr at hensynet til selve saken – og Datatilsynets omdømme som forvalter av nasjonale personverninteresser – fører til at regelhåndhevingen preges av andre virkemidler enn bare kontroller og sanksjoner, først og fremst informering og veiledning. Konsekvensen av dette er at selv om Datatilsynets kontrollvirksomhet er styrket etter at personopplysningsloven og forskriften trådte i kraft (1. januar 2001), har Datatilsynet også rustet opp sin informasjons- og veiledningsaktivitet. Eksempler på dette er at Informasjonsavdelingen har fått flere medarbeidere, det er satset systematisk på å utvikle Datatilsynets hjemmesider på Internett[21] og det er etablert en svartjeneste for telefon- og e-posthenvendelser fra publikum.[22]

I tillegg til kontroller og sanksjoner, informering og veiledning omfatter Datatilsynets virkemiddelarsenal en rekke andre håndhevingsredskaper, for eksempel behandling av søknader om konsesjon for bruk av sensitive personopplysninger, meldeplikt for behandling av ikke-sensitive personopplysninger, områdeovervåkning (følge utviklingen på personvern- og informasjonssikkerhetsfeltet) og ordningen med virksomhetsinterne personvernombud.[23] I drøftelsen nedenfor vil alle disse virkemidlene bli viet oppmerksomhet. Fremstillingen vil isteden fokusere på de to viktigste virkemidlene som Datatilsynet benytter i håndhevingen av bestemmelsene om informasjonssikkerhet: kontroller og sanksjoner, informering og veiledning.

20 «Datatilsynet kan ikke og må ikke opptre som et alminnelig datapoliti (…) utgangspunktet må være at man stoler på individet til det motsatte er kommet frem. Det er gjennom den konstruktive dialog at Datatilsynet har høstet de beste resultat i personvernets navn» (Johansen et al. 2001: 302).

21 Her presenteres nyhetssaker og et relativt omfattende veiledningsmateriale. I tillegg kan enkeltpersoner og virksomheter abonnere på Datatilsynets nyhetsbrev som sendes ut på e-post.

22 Denne tjenesten – Frontservice – bemannes av fire jurister.

23 Personombudsordningen er regulert i personopplysningsforskriften § 7-12, men ordningen er frivillig. Et personvernombud er som regel en ansatt i virksomheten. Ombudets oppgave er å føre oversikt over virksomhetens behandling av personopplysninger og å bidra til at bestemmelsene i regelverket overholdes (se Datatilsynets veileder *Personvernombud. Ombudets rolle og arbeidsoppgaver*, 2007).

Reglene om informasjonssikkerhet

Reglene for sikring av personopplysninger finnes i personopplysningslovens § 13 og i personopplysningsforskriftens kapittel 2.[24] Som de øvrige bestemmelsene i loven og forskriften har de som formål å unngå krenkelser av personvernet (spesielt privatlivets fred og den personlig integriteten) ved behandlingen av personopplysninger.[25] Kravet til informasjonssikkerheten er at den skal være tilfredsstillende, og kommunene må selv avgjøre hva som menes med dette. Hvis kommunene finner at personopplysningene ikke er tilfredsstillende sikret, skal det iverksettes tiltak (tekniske, organisatoriske, bygningstekniske eller personalmessige) for å verne dem mot tre typer sikkerhetsbrudd:

- Brudd på konfidensialiteten: personopplysninger blir gjort kjent for andre enn de som er gitt, og har tjenestelige behov for, tilgang til dem.
- Brudd på integriteten: personopplysninger endres (eller manipuleres) av andre enn de som har fullmakt til å foreta endringer.
- Brudd på tilgjengeligheten: personopplysninger er ikke tilgjengelige for de som er gitt, og har tjenestelige behov for, tilgang til dem.

I tillegg er det gitt regler for hvordan arbeidet med å unngå brudd på opplysningenes konfidensialitet, integritet og tilgjengelighet skal organiseres og gjennomføres. Disse reglene baserer seg på prinsippet om risikostyring.[26] Risikostyrt informasjonssikkerhetsarbeid betyr at kommuner (eller andre virksomheter) selv pålegges å ta stilling til hvor mye sikkerhet som er nødvendig, vurdere hvilke tiltak som bør iverksettes for å oppnå den nødvendige sikkerheten og å kontrollere at tiltakene gir de planlagte resultatene. Dette innebærer en erkjennelse av at kunnskapen som trengs for å tilpasse kravene i regelverket til lokale forhold og behov, ikke forvaltes av embetsmenn i Oslo, men av de ansatte i hver enkelt kommune.

Spørsmålet som drøftes nedenfor er hvordan Datatilsynet benytter kontroller og sanksjoner, informering og veiledning for å håndheve regler hvor kommunene nyter stor frihet til selv å avgjøre hva som er mest hensiktsmessig å gjøre?

---

24 Reglene om informasjonssikkerhet er en forenklet versjon av Den Internasjonale Standardiseringsorganisasjonens (ISO) anbefalinger for organisering og utføring av informasjonssikkerhetsarbeid (se ISO-standard 27002 2005).

25 Personopplysningsloven § 1. Se også Schartum og Bygrave 2004: kapittel 2.

26 Se Schartum 2005 eller Johansen et al. 2001: 128-133 og 344-357. For nærmere diskusjoner av risikostyring og organisering av informasjonssikkerhetsarbeidet, se for eksempel Slay og Koronios 2006, Daler et al. 2002: 121-142, Schneier 2000: 301-302 eller Saltmarsh og Brown 1983.

Kontroller og sanksjoner

Mens Datatilsynets arbeid på 1980-tallet var preget av liten kontrollvirksomheten og omfattende saksbehandling (konsesjonssaker),[27] økte antallet kontroller noe utover på 1990-tallet: I 1996 ble det gjennomført 28 stedlige kontrollbesøk, mens 23 kontrollbesøk ble gjennomført i 1999. I 2001 hadde antallet kontroller steget til 53, noe som henger sammen med at personopplysningsloven med forskrift trådte i kraft dette året.[28] En av de viktigste forskjellene i forhold til den gamle personregisterloven (som gjaldt fra 1980 og frem til 1. januar 2001), er at konsesjonsordningen har en mindre sentral plass i den nye loven.[29] Fremfor styring i forkant gjennom konsesjonsbehandling, legges det nå større vekt på kontroll i etterkant. Internt i Datatilsynet fikk dette som konsekvens at en egen Tilsyns- og sikkerhetsavdeling ble opprettet i 2001.[30] Utover på 2000-tallet fortsatte derfor kontrollvirksomheten å vokse – til 141 kontrollbesøk i 2008.[31]

Selv om kontrollvirksomheten har økt de siste 8-10 årene, har avdelingen i Datatilsynet som er ansvarlig for denne virksomheten – Tilsyns- og sikkerhetsavdelingen – bare åtte ansatte. Det betyr at kontrollkapasiteten er begrenset,[32] og for å utnytte den så effektivt som mulig er utvelgelsen av tilsynsobjekter

27 Se Seip 1990 og Føyen 1989.

28 Se Datatilsynets årsmeldinger for 1996, 1999 og 2001.

29 I motsetning til tidligere, er det bare nødvendig å søke konsesjon for behandling av sensitive personopplysninger. Behandling av ikke-sensitive personopplysninger er underlagt meldeplikt (se personopplysningsloven kapittel 6). Meldepliktsystemet skal gi Datatilsynet informasjon om hvem som behandler hvilke typer personopplysninger og til hvilke formål. Denne informasjonen er bl.a. ment å føre til at kontrollvirksomheten utføres på en mer målrettet og effektiv måte.

30 Konsekvensene av overgangen til et nytt regelverk, er drøftet i en relativt omfattende organisasjonsutredning fra 2001 (*En organisasjon tilpasset Datatilsynets nye oppgaver i et samfunn i endring*, november 2001). Her ble behovet for å styrke kontrollkapasiteten løftet fram som en spesielt viktig utfordring.

31 *Datatilsynets årsmelding for 2008*, s. 24. En annen årsak til økningen i kontrollvirksomheten, er at i tildelingsbrevet fra FAD ble Datatilsynet pålagt å gjennomføre minst 130 kontrollbesøk i året. Dette måltallet er nå fjernet, men det understrekes fortsatt at Datatilsynet skal satse på å styrke kontrollvirksomheten.

32 Begrensninger i kontrollkapasiteten fører for eksempel til at Datatilsynet mangler ressurser til å gjennomføre etterkontroller av hvordan kommuner (og andre virksomheter) følger opp pålegg om retting av regelavvik.

basert på risikovurderinger.[33] Risikoutvelgelse av tilsynsobjekter innebærer at stedlige kontroller gjennomføres overfor virksomheter i sektorer eller bransjer som antas å være spesielt utsatt for brudd på informasjonssikkerheten (eller hvor de personvernmessige konsekvensene av sikkerhetsbrudd antas å være særlig alvorlige). Kommunene står derfor høyt på Datatilsynets prioriteringsliste, bl.a. fordi de behandler store mengder sensitive personopplysninger (for eksempel helsedata). Dette har gitt seg utslag i at siden personopplysningsloven og forskriften trådte i kraft, har flere stedlige kontroller vært gjennomført i kommunesektoren enn i de fleste andre bransjer eller sektorer.

Begrenset kontrollkapasitet fører bl.a. til at Datatilsynet ser det som ekstra viktig å være tydelig på hvilke regelbrudd kommunene har gjort seg skyldig i og hva de må gjøre for å være i tråd med regelverket. Datatilsynet nøyer seg derfor ikke med å bruke de mildeste sanksjonsformene – for eksempel påpekning av regelbrudd – men fatter vedtak som innebærer en rettslig plikt til å rette de regelavvikene som oppdages. Hyppigheten i bruken av formelle vedtak fremgår av Datatilsynets kontrollrapporter fra kommunesektoren for perioden 2001 til 2008. Her viser det seg at pålegg om retting av regelavvik ble fattet ved over 90 % av kontrollbesøkene, og at påleggene i særlig grad rettet seg mot brudd på reglene om informasjonssikkerhet. Kontrollrapportene viser samtidig at det bare var i ett tilfelle hvor det kommunale informasjonssikkerhetsarbeidet ble oppfattet som så mangelfullt at en strengere reaksjonsform enn pålegg om retting av avvik ble vurdert.[34]

Begrensninger i kontrollkapasiteten innebærer at kontroller og sanksjoner ikke benyttes uavhengig av andre virkemidler. I interne strategidokumenter fremheves det for eksempel at Datatilsynets mediearbeid bør planlegges i forbindelse med utarbeidelsen av de årlige tilsynsplanene.[35] Tanken er at kontrollfunn fra kommunesektoren (men også fra andre sektorer og bransjer) skal

33 Mer målrettet innsats mot spesielt risikoutsatte bransjer eller sektorer er viktig fordi kontrollkostnadene er betydelige og omfatter en rekke aktiviteter: utvelgelse av tilsynsobjekter, sammensetning av tilsynsteam og fordeling av tilsynsobjekter, utsending av varsel om kontroll, innhenting og gjennomgang av skriftlig materiale tilsendt fra tilsynsobjektene, gjennomføring av selve kontrollen, analyse av kontrollfunn og utarbeidelse av foreløpig og endelig kontrollrapport. Dessuten er kontrollvirksomheten forbundet med en del indirekte kostnader, for eksempel at saksbehandlingskapasiteten i Juridisk avdeling svekkes når jurister deltar i kontrollarbeidet.

34 Etter at personopplysningsloven med forskrift trådte kraft, har verken tvangsmulkt eller politianmeldelse vært benyttet i kommunesektoren eller for brudd på reglene om informasjonssikkerhet.

35 Se *Strategi og metodikk for operativt tilsyn med behandling av personopplysninger*, 2002, s. 11-13.

brukes som «råstoff» i Datatilsynets mediearbeid.[36] Dette skal bl.a. synliggjøre at Datatilsynet gjennomfører kontroller og ilegger sanksjoner, og bidra til at informasjonssikkerhet settes på den kommunale dagsorden.[37] Offentliggjøring av kontrollfunn kan også tenkes å ha en viss allmennpreventiv virkning: Ved at det gjøres oppmerksom på at regelpraksis kontrolleres, og ved at det gis informasjon om at regelbrudd sanksjoneres, sendes et signal til alle kommuner om at de bør ta reglene om informasjonssikkerhet på alvor.

Men kontrollvirksomheten tjener ikke bare en avskrekkingsfunksjon fordi den også er Datatilsynets viktigste kommunikasjonskanal ut mot kommunene (og andre sektorer eller bransjer). Kontrollbesøk gjør at Datatilsynet kommer i direkte inngrep med kommunene: tilsynsorganet får anledning til å informere om og diskutere regelverket med de som skal følge det. Stedlige kontroller kan derfor hjelpe kommunale IT- og sikkerhetsledere med å løse forankringsproblematikken, det vil si å forklare betydningen av informasjonssikkerhet og personvern overfor kommunenes administrative toppledelse (rådmennene). Samtidig har kontrollvirksomheten betydning for kompetanseoppbyggingen internt i Datatilsynet. På den ene siden fører stedlige kontroller til at Datatilsynet får oppdatert sin kunnskap om hvilke tekniske og organisatoriske utviklingstrekk som preger det kommunale informasjonssikkerhetsarbeidet. På den andre siden bidrar kontrollene til å identifisere problemstillinger som Datatilsynet tidligere ikke har tatt stilling til. Kontrollene er derfor avgjørende for dannelsen av ny forvaltningspraksis.

Informering og veiledning

Målet med Datatilsynets informasjons- og veiledningsarbeidet er at kommunene (og andre pliktsubjekter) skal internalisere reglene om informasjonssikkerhet: lokale myndigheter skal settes i stand til å praktisere regelverket på en måte som gjør at det blir en naturlig del av de daglige gjøremålene.[38] Informasjons- og veiledningsarbeidet på informasjonssikkerhetsområdet har derfor en noe annen innretning enn Datatilsynets øvrige informasjons- og vei-

36 Se spesielt Datatilsynets strategidokument for medie- og kommunikasjonsarbeidet: *Kommunikasjon for et bedre personvern 2007-2010* (2006).

37 Se *Strategi og metodikk for operativt tilsyn med behandling av personopplysninger*, 2002, s. 11-13. Aktiv bruk av bransjeblader eller tidsskrifter fremheves som en særlig effektiv måte å kommunisere kontrollfunn på – og å meddele kommunesektoren at Datatilsynet holder et våkent øye med hva den foretar seg.

38 Troen på at veiledning og opplæring kan ha en internaliseringseffekt, er noe større i Informasjonsavdelingen enn i Tilsyns- og sikkerhetsavdelingen. Holdningen i Tilsyns- og sikkerhetsavdelingen er at veiledning og opplæring ikke vil gi en slik effekt uten bruk av kontroll- og sanksjonsvirkemidler.

ledningsarbeide. Istedenfor å opplyse om trusler mot og viktigheten av personvern, handler det om å operasjonalisere regelverket, det vil si å forklare hva risikostyrt informasjonssikkerhetsarbeid i praksis innebærer. Til dette formålet har Datatilsynet utarbeidet en rekke veiledere og kommentarhefter som utdyper innholdet i lov- og forskriftsteksten,[39] og som gir konkrete eksempler på hvordan virksomheter kan gå frem for å overholde bestemmelsene.[40] Det er også laget en egen veileder om informasjonssikkerhet spesielt rettet mot kommunesektoren.[41]

I tillegg (og som nevnt ovenfor) er bruken av informerings- og veiledningsvirkemidler intimt koblet til Datatilsynets kontrollvirksomhet. Denne koblingen kommer til uttrykk ved at den hyppigst brukte sanksjonen for brudd på informasjonssikkerhetsreglene i kommunesektoren – pålegg om retting av regelavvik – like gjerne kan forstås som en juridisk bindende form for rådgivning som en straffereaksjon. Dette innebærer at Datatilsynets stedlige kontroller neppe kan forstås som kortvarige enkelthendelser hvor hensikten utelukkende er å oppdage og korrigere regelavvik. Kontrollene kan også legge grunnlaget for gjentatt samhandling mellom tilsynsorgan og tilsynsobjekt, for eksempel ved at kommuner som pålegges å rette regelavvik henvender seg til Datatilsynet for å få råd (formidlet via oppfølgingsmøter, telefonsamtaler eller e-postkommunikasjon) om hva de bør gjøre for å utbedre manglene. På denne måten blir håndhevingen av sikkerhetsbestemmelsene like mye en (ressurskrevende) prosess som isolerte og enkeltstående hendelser.

Den intime koblingen mellom kontrollvirksomheten og informerings- og veiledningsarbeidet, gjør at Datatilsynet er opptatt av å unngå rollemotsetninger. Datatilsynet som regelkontrollør ønsker derfor ikke å komme i konflikt med Datatilsynet som veileder, for eksempel ved at kommunene forklarer regelbrudd med at de bare har gjort som Datatilsynet selv anbefaler. Denne typen rollemotsetninger blir forsøkt løst ved at tilsynsorganet unngår å gi svært

39 Se *Internkontroll og informasjonssikkerhet* (2007), *Internkontroll i mindre virksomheter – introduksjon* (2007), *Internkontroll i mindre virksomheter – eksempler* (2007), *Risikovurdering av informasjonssikkerhet* (2002) og *Sikkerhetsbestemmelsene i personopplysningsloven* (2000).

40 Veiledningsmaterialet inneholder bl.a. forslag til hvordan sikkerhetsdokumenter (sikkerhetsmål og strategier, sikkerhetsinstrukser, taushetserklæringer, avviksrapporteringsskjema, osv.) kan utformes.

41 Se *Veiledning i informasjonssikkerhet for kommuner og fylker* (2005). Ifølge en kartlegging utført av Rambøll Management Consulting på oppdrag fra Kommunenes Sentralforbund, rapporterer 80 % av kommunene at de følger Datatilsynets informasjonssikkerhetsanbefalinger (Kommunal Rapport 26. mai 2009). Datatilsynets kontrollrapporter indikerer at selv om kommunene baserer seg på tilsynsorganets anbefalinger, er det langt igjen til at anbefalingene følges (se nedenfor og Tranvik 2010b).

detaljerte råd til kommunene om hvilke konkrete sikringstiltak de bør iverksette. Datatilsynet anbefaler for eksempel ikke bestemte sikkerhetsteknologier og setter ikke sitt godkjenningsstempel på lokale risikovurderinger.[42] Slike anbefalinger eller godkjenninger vil ikke bare føre til at Datatilsynet risikerer å møte seg selv i døra når det er på stedlige kontroller. Det bryter også med forutsetningen som informasjonssikkerhetsbestemmelsene hviler på, nemlig at kommunene selv – med bakgrunn i egne vurderinger – skal avgjøre hvor mye sikkerhet som er nødvendig og hvilke tiltak som gir den ønskede sikkerheten.

Samarbeid med sektorrepresentanter

Samarbeid med sektorrepresentanter utgjør en stadig viktigere del av Datatilsynets informerings- og veiledningsarbeid. Dette kommer til uttrykk både på informasjonssikkerhetsområdet og i kommunesektoren. Særlig viktig har Datatilsynets støtte til Foreningen for kommunal informasjonssikkerhet (KINS) vært. KINS er en frivillig organisasjon som primært er ment å være en møteplass for ansatte i kommuner og fylkeskommuner som jobber med informasjonssikkerhetsspørsmål.[43] Datatilsynet spilte en aktiv rolle da KINS ble opprettet i 2003, og har senere bidratt med støtte til foreningen (bl.a. ved å stille med foredragsholdere på møter og konferanser). I tillegg har Datatilsynet møte- og talerett i foreningens styre. Samarbeidet med Kommunenes Sentralforbund – hvor KS IKT-forum[44] er en naturlig partner – har imidlertid vært relativt beskjedent. Det kan skyldes at KINS har fungert såpass bra som inngangsport mot kommunene (i alle fall når det gjelder informasjonssikkerhet) at utstrakt samarbeid med KS ikke har vært nødvendig.

I tillegg til bransje- og sektororganisasjoner, forsøker Datatilsynet å etablere dialog med, og drive informerings- og veiledningsvirksomhet overfor, leverandører av IT-systemer. Problemet, ifølge Datatilsynet, er at mange leverandører tenker funksjonalitet og brukervennlighet snarere enn informasjonssikkerhet når nye IT-systemer planlegges og utvikles. Det hevdes å føre til to ting. For det første at lovgivningens krav om tilfredsstillende sikring

42 Men Datatilsynet har likevel myndighet til å gripe inn i det lokale informasjonssikkerhetsarbeidet. I personopplysningsforskriften § 2-2 heter det for eksempel at Datatilsynet kan overprøve kommuners (og andre virksomheters) egen definisjon av hva som menes med tilfredsstillende informasjonssikkerhet. Denne myndigheten har ikke Datatilsynet benyttet, bl.a. fordi det risikerer å føre kontroll med sine egne anbefalinger.

43 KINS hadde ved utgangen av 2008 omkring 90 kommuner og fylkeskommuner som medlemmer, se www.kins.no.

44 KS IKT-forum har som formål å styrke e-forvaltnings- og teknologiarbeidet i kommuner og fylkeskommuner, se www.ksikt-forum.no.

av personopplysninger blir vanskelig å ivareta (leverandørene lar sikkerheten vike til fordel for andre hensyn). For det andre at når leverandørene nedprioriterer informasjonssikkerhet, legges kostnadene knyttet til sikring av usikre IT-systemer over på kommunene. Hvert år har derfor Datatilsynet en rekke møter med teknologibransjen hvor det informeres om lovgivningens krav til informasjonssikkerhet.[45] Det er imidlertid usikkert hvorvidt møtene har betydning for om lovkrav legges til grunn ved utformingen av nye IT-systemer.[46]

Effekter av virkemiddelbruken

Hvilken innvirkning har Datatilsynets virkemiddelbruk – anvendelsen av kontroller og sanksjoner, informering og veiledning – hatt på kommunenes etterlevelse av personopplysningslovens og forskriftens bestemmelser om informasjonssikkerhet?

Å måle effekter av ulike typer virkemidler er en usikker affære, både fordi endringer i graden av regeletterlevelse kan være problematisk å påvise og fordi det er vanskelig å knytte eventuelle endringer til Datatilsynets virkemiddelbruk (det vil si at det kan være komplisert å skille effektene av Datatilsynets virkemiddelbruk fra andre forhold som også kan påvirke graden av kommunal regeletterlevelse). Likevel kan Datatilsynets rapporter fra stedlige kontroller av kommunenes regelpraksis, gjennomførte i perioden 2001 til og med 2008, gi visse indikasjoner.[47] I kontrollrapportene fremgår særlig to forhold.

For det første at prosentandelen kontrollbesøk hvor det gis pålegg om retting av regelavvik ikke har gått ned i løpet av perioden (andelen ligger stabilt på ca. 90 % pr. år, og i enkelte år er den oppe i 100 %). For det andre at Datatilsynet gir like mange pålegg om retting av regelavvik pr. kontrollbesøk i perioden 2006-08 som i perioden 2001-05. Begge disse forholdene synes å indikere at den kommunale regeloverholdelsen – og effektene av Datatilsynets virkemiddelbruk – ikke har endret seg vesentlig siden bestemmelsene om informasjonssikkerhet trådte i kraft.

45 Det er ikke bare Datatilsynet som tar initiativ til disse møtene, men det hender at IT-leverandørene selv ber om råd for hvordan IT-systemer kan utvikles slik at lovgivningens krav ivaretas. Liknende veiledningsmøter gjennomføres med representanter for konsulentbransjen.

46 Datatilsynet har også gjennomført kontroller med hvordan de delene av teknologibransjen som leverer løsninger til kommunene overholder informasjonssikkerhetsbestemmelsene (for eksempel leverandører av skjemamotorer til kommunene).

47 Det kan være problematisk å basere seg på kontrollrapporter for å vurdere effektene av virkemiddelbruken. Kontrollrapportene gir for eksempel få holdepunkter for å vurdere om pålagte rettinger av regelavvik faktisk gjennomføres fordi etterkontroller ikke foretas.

Men hvis vi analyserer hvilke pålegg Datatilsynet gir, ser bildet litt annerledes ut. Da viser det seg at mens det fra 2001 til 2005 ikke var uvanlig at ett enkelt pålegg omfattet brudd på flere ulike bestemmelser, har det de to-tre siste årene blitt vanligere å gi individuelle pålegg for hvert regelbrudd. Dermed synker ikke antallet pålegg pr. kontrollbesøk fordi påleggene er blitt mer detaljerte og spesifikke. Dette kan bety at virkemiddelbruken har gitt resultater fordi typen pålegg som gis antyder at regelbruddene er mindre omfattende enn tidligere. Men det kan også skyldes andre forhold, for eksempel at kommunene har trengt tid til å komme i gang med implementeringsarbeidet. En tredje forklaringsmulighet er at Datatilsynets kontroller har endret karakter: de er blitt mer detaljorienterte. Datatilsynet fører i økende utstrekning kontroll med overholdelsen av spesifikke bestemmelser i regelverket snarere enn med systematikken i kommunenes generelle informasjonssikkerhetsarbeid. Det kan følgelig tenkes at endringene i vedtakenes form avspeiler endringer i Datatilsynets virkemiddelbruk, men sier mindre om den faktiske utviklingen i kommunenes regeletterlevelse.

Vanskeligheten med å knytte endringer i regeloverholdelsen til Datatilsynets virkemiddelbruk fremgikk også av intervjuer med IT- og sikkerhetsledere i 19 store og mellomstore kommuner på østlandsområdet. Her ble tre forhold nevnt. For det første ble det hevdet at fokuset på å følge regelverket varierte over tid. Stedlige kontroller hadde for eksempel en positiv, men kortsiktig virkning på regeloverholdelsen. Etter hvert som tiden tilbake til det siste kontrollbesøket økte, var det en tendens til at oppfølgingen av reglene fortok seg. For det andre ble det hevdet at regeloverholdelsen varierte mellom kommunale virksomhetsområder. Innenfor helse- og omsorgssektoren fikk regelverket størst oppmerksomhet, mens skole ble av mange sett på som et problemområde. For det tredje ble enkelte bestemmelser overholdt i større grad enn andre. Spesielt kravene til organisering av sikkerhetsarbeidet og utarbeidelse av plandokumenter (sikkerhetsmål, sikkerhetsstrategi, akseptkriterier og rutiner for sikkerhetsarbeidet) ble overholdt, men de øvrige bestemmelsene – selve praktiseringen av planverket – ble ikke prioritert like sterkt. Disse forholdene gjør det problematisk å si noe generelt og presist om endringer i graden av regeloverholdelse, og dermed også om effekten av Datatilsynets virkemiddelbruk.

Avslutning

Drøftelsene i denne artikkelen har vist at håndhevingen av personopplysningslovens og forskriftens regler om informasjonssikkerhet er ressurskrevende: det fordrer betydelig informerings-, veilednings- og kontrollinnsats fra Datatilsynets side. Den har også vist at kontroller og sanksjoner er virkemidler

som har fått større betydning i Datatilsynets håndhevingsarbeid enn tidligere. Men, på den annen side, er Datatilsynets bruk av informerings- og veiledningsvirkemidler også styrket. I tillegg er bruken av de to virkemiddeltypene relativt tett integrert, for eksempel ved at stedlige kontroller ikke bare benyttes for å oppdage og korrigere regelbrudd, men samtidig er en anledning til å formidle råd og veiledning til tilsynsobjektene. Vi har også sett at virkemiddelbruken påvirkes av Datatilsynets kontroll- og veiledningskapasitet – den fremstår som underdimensjonert i forhold til tilsynsorganets store ansvarsområde.

I hvilken grad har Datatilsynets virkemiddelbruk ført til økt kommunal regeloverholdelse? De empiriske funnene fra kommunesektoren viser to ting:

- Datatilsynet gir ikke færre pålegg om retting av regelavvik i perioden 2006-08 enn i årene like etter at bestemmelsene om sikring av personopplysninger trådte i kraft.
- Kommunenes regeloppfølging synes å skje stykkevis og delt: den varierer fra et tidspunkt til et annet, den varierer på tvers av kommunale virksomhetsområder og den varierer mellom de ulike bestemmelsene i regelverket.

Med bakgrunn i disse funnene synes det vanskelig å finne belegg for at Datatilsynets virkemiddelbruk i betydelig grad har påvirket kommunenes praktisering av bestemmelsene om informasjonssikkerhet. Men funnene er usikre og nærmere empiriske analyser er nødvendig for å sannsynliggjøre eller avkrefte denne konklusjonen.

Litteratur

Baldwin, Robert et al. (red.) (1998): A Reader on Regulation. Oxford: Oxford University Press.

Daler, Torgeir et al. (2002): Håndbok i datasikkerhet. Informasjonsteknologi og risikostyring. Trondheim: Tapir akademiske forlag.

Føyen, Arve (1989): *Datatilsynet*. I Guttorm Hansen et al. (red.): Mennesket i sentrum. Festskrift til Helge Seips 70-årsdag. Oslo: Tano.

Johansen, Michal Wiik et al. (2001): Personopplysningsloven. Kommentarutgave. Oslo: Universitetsforlaget.

Saltmarsh, Timothy J. og Peter S. Browne (1983): *Data Processing – Risk Assessment*. I Marvin M. Wofsey (red.): Advances in Computer Security Management. Chichester: John Wiley.

Schartum, Dag Wiese (2005): *Krav til sikring av personopplysninger*. I Arild Jansen og Dag Wiese Schartum (red.): Informasjonssikkerhet. Rettslige krav til sikker bruk av IKT. Bergen: Fagbokforlaget.

Schartum, Dag Wiese og Lee A. Bygrave (2004): Personvern i informasjonssamfunnet. En innføring i vern av personopplysninger. Bergen: Fagbokforlaget.

Schneier, Bruce (2000): Secrets and Lies. Digital Security in a Networked World. New York: John Wiley.

Seip, Helge (1990): *Ti år med Datatilsynet*. I Eirik Djønne (red.): 10 år som personvernets vokter. Oslo: Tano.

Slay, Jill og Andy Koronios (2006): Information Technology Security and Risk Management. Sydney: John Wiley.

Tranvik, Tommy (2010a): Kommunal regeletterlevelse. Realiteter og illusjoner på personvernområdet (til publisering).

Tranvik, Tommy (2010b): Avskrekking eller etterlevelse? Datatilsynets virkemiddelbruk overfor kommunene (til publisering).

Andre kilder

Datatilsynet (2009): Datatilsynets årsmelding 2008.

Datatilsynet (2007): Personvernombud. Ombudets roller og arbeidsoppgaver.

Datatilsynet (2007): Internkontroll og informasjonssikkerhet.

Datatilsynet (2007): Internkontroll i mindre virksomheter – introduksjon.

Datatilsynet (2007): Internkontroll i mindre virksomheter – eksempler.

Datatilsynet (2006): Kommunikasjon for et bedre personvern 2007-2010.

Datatilsynet (2005): Veiledning i informasjonssikkerhet for kommuner og fylker.

Datatilsynet (2002): Strategi og metodikk for operative tilsyn med behandling av personopplysninger.

Datatilsynet (2002): Datatilsynets årsmelding 2001.

Datatilsynet (2002): Risikovurdering av informasjonssikkerhet.

Datatilsynet (2001): En organisasjon tilpasset Datatilsynets nye oppgaver i et samfunn i endring.

Datatilsynet (2000): Datatilsynets årsmelding 1999.

Datatilsynet (2000): Sikkerhetsbestemmelsene i personopplysningsloven.

Datatilsynet (1997): Datatilsynets årsmelding 1996.

Kommunal Rapport, 26. mai 2009

NOU (2009: 1): Individ og integritet. Personvern i det digitale samfunnet.

Personopplysningsloven – Lov om behandling av personopplysninger (personopplysningsloven) av 14.april 2000 nr 31.

Personopplysningsforskriften - Forskrift om behandling av personopplysninger (personopplysningsforskriften) av 15.desember 2000 nr 1265.

IT-STØTTE FOR LOVSAKER (LOVIT)[1]

Dag Wiese Schartum

1 Systemutvikling som regelverksutvikling

Et av elementene i masterstudiet i forvaltningsinformatikk er «systemutvikling som regelverksutvikling». Utgangspunktet er erfaringer fra arbeidet med automatisering av enkeltsaksbehandlingen innen forvaltningsområder med klart definerte regelverk (skatt, trygd, avgift mv). Slik automatisering krever at regelverket fortolkes og uttrykkes ved hjelp av programmeringsspråk. Det er imidlertid ikke selve programmeringen og den etterfølgende automatiserte saksbehandlingen som er av interesse når systemutvikling ses som regelverksutvikling: For å kunne programmere rettsregler må man gjøre en omfattende analyse av lovteksten, og denne analysen kan brukes for to ulike formål. Én anvendelse er å utvikle systemløsninger for helt eller delvis å automatisere saksbehandlingsarbeidet. Den andre anvendelsen innebærer å tilbakeføre analyseresultatene til lovteksten og dermed - muligens - forbedre denne.

Systemutvikling som regelverksutvikling går i korte trekk ut på å gjennomføre formelle analyser av et foreliggende regelverk med det formål å avdekke og utnytte forbedringsmulighetene. Analyseresultatene anvendes for å gjøre rettsreglene i naturlig språk («vanlig norsk») bedre, *ikke* for å endre til et norsk som ligner datamaskinprogram. Stikkord i analysen er særlig struktur, konsistens og konsekvens. En vil for eksempel være opptatt av konsistent og konsekvent bruk av sentrale begreper. Dersom «inntekt», «arbeidsinntekt» og «lønn» brukes i samme regelverk, vil kravet være at variasjonen har rettslig begrunnelse og betydning. Videre vil en være opptatt av å kartlegge de logiske og aritmetiske strukturene i regelverket, og påse at vilkårsstrukturer og regneregler mv er uttrykt på utvetydig måte. Også spørsmål om sekvens og etablering av forløp vil være viktig. For eksempel vil rettsreglene, om mulig, settes opp i den rekkefølge de typisk skal utføres, og/eller en vil være opptatt av å angi klare «adresser» for å angi hvilke regelelementer som må utføres i rekkefølge. Poenget er at regelverket ikke skal framstå som mer fragmentert enn nødvendig.

Det er flere teknikker og hensyn enn de som er nevnt her som inngår i masterstudentenes bestrebelser på å skrive om lovbestemmelser mv slik at de blir

1 Artikkelen er basert på artikkel i Lov&Data nr 97, mars 2009, s. 20-23. Siste avsnitt er nyskrevet.

lettere å forstå og anvende uten vesentlig å endre på det materielle innholdet. Formålet her er imidlertid ikke å forklare hva slike analysearbeider går ut på, men å fremheve det som fremstår som en alminnelig erfaring fra slike arbeider; *at potensialet for å forbedre lov- og forskriftstekster er stort*. Selvsagt skrives det også lover med høy kvalitet. Likevel er det etter min mening grunn til å spørre seg hvordan situasjonen kan forbedres og om arbeidet med utarbeidelse av lover kan gjøres mer hensiktsmessig. En forvaltningsinformatiker vil straks tenke at et *IT-verktøy*, dvs. et informasjonssystem til bruk i arbeidet med lover, må være en del av svaret.

2 Bruk av IT i lovarbeider «på vanlig måte»

Dagens samfunn er så gjennomsyret av informasjons- og kommunikasjonsteknologi og elektroniske løsninger at «e»er vi setter foran mange ord for å minne om elektronikkens rolle snart er moden for sanering. En av de meget få områdene der IT/IKT *ikke* blir brukt på spesialiserte måter er innen regelverksutvikling, dvs som ledd i utarbeidelsen av lover og forskrifter. I prosjektet «IT-støtte for arbeid med lovsaker» (LovIT)[2] var de gjennomgående svarene fra utvalgsledere og -sekretærer at IT i lovgivningsarbeider ble brukt «på vanlige måte». Jeg er redd dette betyr at IT-bruken ikke var særlig gjennomtenkt. Mer konkret betyr det at tekstbehandling, epost, Lovdata, Regjeringen.no mv blir brukt slik deltakerne er vant til i andre situasjoner - uten at teknologien er spesielt utformet ut i fra de krav lovgivningsarbeidet stiller. I Norge finnes det ikke noe IT-verktøy for lovmakere, bare noen enkle tekstbehandlingsmaler for oppsett av NOU-tekster mv. Ut i fra kompleksiteten og betydningen av lovgivningsarbeider er denne manglende bevisstheten om og tilgangen til IT-verktøy overraskende.

Hva kan gjøres? Her er det bare mulig å beskrive noen få av de mange mulige støttefunksjoner som et lovgivningsverktøy kan inneholde. For øvrig viser jeg til kapittel 3 i LovIT-rapporten.[3] Blant de muligheter som foreligger går det et skille mellom slike som tilsvarer innhold i Lovteknikk-heftet og muligheter ut over dette. Heftet «Lovteknikk» er en veiledning for lovarbeid vedrørende utforming av lovtekster mv, og er utarbeidet av Lovavdelingen i Justis- og politidepartementet. Teksten er også tilgjengelig fra Regjerningen.no. Forslagene i LovIT-rapporten gjelder dels spørsmål som ikke er omhandlet i Lovteknikk, og dels spørsmål som kun er beskrevet i sakprosa men som kan programmeres og gjøres tilgjengelig som *funksjoner*.

2 Se http://www.jus.uio.no/ifp/seri/forskning/prosjekter/lovit/.

3 Se Dag Wiese Schartum, It-støtte for arbeid med lovsaker, Complex 4/08, Senter for rettsinformatikk, Oslo 2008, også tilgjengelig fra http://www.jus.uio.no/forskning/prosjekter/lovit/.

3 IT-bruk ved oppstart av lovarbeider og grunnleggende struktur for teknologistøtten

Dersom en skal legge bedre til rette for lovgivningsarbeider ved hjelp av IT, er det aller enkleste og mest åpenbare å gjøre aktuelle tekster som skal ligge til grunn for et lovarbeide tilgjengelige i maskinlesbar form på en enhetlig måte. Alle lovutredere skal for eksempel forholde seg til et mandat, regelverksinstruksen og Lovteknikk-heftet, og ofte er de også pålagt å bruke NOU-malen (som styrer oppsett av manus slik det skal trykkes). I tillegg kommer diverse Stortingsdokumenter mv som utgjør bakgrunn for arbeidet, samt Justisdepartementets veiledere for utvalgsledere og -sekretærer. I de to lovutvalgene jeg undersøkte i LovIT-prosjektet var kunnskapen om slike dokumenter varierende og tilgangen til dels tilfeldig. Det er nærliggende å spørre hvorfor slike dokumenter ikke gjøres tilgjengelige i maskinlesbar form på standardisert måte ved *hver* oppnevnelse av lovutvalg - for eksempel innenfor rammene av et nettsted for hvert lovutredningsarbeid?

I sentrum bør det etter min mening være et nettsted med standardisert struktur som alltid opprettes i tilknytning til igangsetting av et lovgivningsarbeid. Delvis bør et slikt nettsted være åpent tilgjengelig for enhver. I tillegg bør lovutvalget ha tilgang på et passordbeskyttet «arbeidsrom» knyttet til nettstedet der arbeidsdokumenter, møtereferater, utkast mv er tilgjengelig. Slike funksjoner vil sikre en felles oversikt for lovutrederne over aktuelt materiale, gi enhetlig versjonskontroll av utkast, og generelt gjøre det mulig å redusere papirhåndteringen fordi alt materialet kan være tilgjengelig på PC i møter mv.

4 Bruk av maler mv

En del av innholdet i Lovteknikk-heftet er anvisninger av hvorledes lovtekst skal/kan settes opp. Dette er spørsmål som det er uhensiktsmessig (bare) å uttrykke som tekst. Hvorfor er det ikke laget tekstbehandlingsmaler som gjennomfører Lovteknikk-heftets beskrivelser av lovlig tekstoppsett? Hvorfor skal det være nødvendig for lovutredere å *manuelt* endre gjennomgående nummerering av paragrafer, bruk av legaldefinisjoner mv i en lovtekst under arbeid? Delvis automatiske funksjoner for gjennomgående endringer av nummereringer, henvisninger og bruk av legaldefinisjoner er en veldig nærliggende forventning. Etter min mening er det også grunn til å gi spesiell støtte for skriving av for eksempel spesielle motiver og dissenser.[4]

4 Se nærmere om dette i LovIT-rapporten s 54 - 55. Referanse til rapporten finnes i fotnote 1.

5 Legaldefinisjoner mv

Legaldefinisjoner er begreper med sentral betydning for formulering av lovens bestemmelser. En vanlig teknikk er å samle slike definisjoner i en bestemmelse tidlig i lovteksten, men definisjoner kan også forekomme i andre deler av teksten. Legaldefinisjoner er ikke sjelden basert på tilsvarende definisjoner i EU-direktiv eller -forordning. Sentrale begreper som ikke er definert i loven vil normalt være omtalt og nærmere definert i merknadene til den enkelte bestemmelse, og også legaldefinisjoner vil ofte være utfyllende definert og presisert i de særlige motivene.

Legaldefinisjonenes sentrale betydning for en lovtekst kan begrunne IT-støtte for å tilrettelegge for gjennomarbeidet og konsistent begrepsbruk. For det første kan det under utarbeidelsen være grunn til å tydeliggjøre hvorledes legaldefinisjoner og andre sentrale begreper er anvendt i lovteksten. En mulighet er å merke alle forekomster av legaldefinisjoner. I tillegg kan ordlyden i definisjonene knyttes til hver forekomst i lovteksten, for eksempel på samme måte som merknadstekster fremkommer i Word. En slik funksjon krever liten arbeidsinnsats men gir forholdsvis mye og potensielt verdifull informasjon til lesere av lovutkast.

Et IT-verktøy kan også brukes til å identifisere begreper som enten bør vurderes for legaldefinering og/eller for særlig utfyllende begrepsmessig avklaring i merknadene til den enkelte bestemmelse, eventuelt i lovens generelle motiver. Kriteriene for identifikasjon av begreper som kan vurderes kan være flere, men det er lettest å tenke seg at enkelte rent språklige og/eller systematiske kriterier i kombinasjon kan gjøres utslagsgivende. For eksempel kan ord som er brukt i et lovutkast være legaldefinert i en annen lov eller forskrift. IT-verktøyet kan settes opp med søkefunksjoner som kartlegger slike definisjoner.

6 Tverrgående begrepsanalyser

I høst la regjeringen fram en rapport om IKT-arkitektur i offentlig sektor,[5] og blant de viktigste punktene var «semantisk interoperabilitet», dvs. ønsket om å kunne ha større grad av tverrgående begrepsdefinisjoner for derved å gjøre det mulig å ha felles opplysningstyper innen ulike deler av forvaltningen. Offentlig forvaltning er i stor grad lovstyrt, og mange begreper er derfor fastsatt som del av lovgivningsprosessen. I hvilke grad ønsker om å felles opplysningstyper kan imøtekommes eller ikke, er med andre ord i stor grad avhengig av lovgivningsmessige valg.

5 Se rapporten «Felles IKT-arkitektur i offentlig sektor», rapport avgitt fra arbeidsgruppe til Fornyings- og administrasjonsdepartementet, 21. desember 2007.

Ofte vil det være gode grunner til å velge ulike definisjoner av samme ord fra en lov til en annen. I andre tilfelle er det imidlertid neppe tilstrekkelig grunn til å velge forskjellig. Et spadestikk i forekomster av begrepet «samboer» i lovgivningen, viste for eksempel at det i fem undersøkte lover er forskjellige men veldig nært beslektede definisjoner av samboerskap.[6] Dersom spørsmålet hadde vært stilt om ulikhetene er vel begrunnet, er det sannsynlig at en god del forskjeller kunne ha vært eliminert. Det er etter min mening grunn til å tro at ubegrunnede forskjeller mellom slike definisjoner kunne ha blitt vesentlig redusert dersom lovutredere hadde et IT-verktøy som la til rette for å søke etter eksisterende forekomster av begreper de vurderer å gi sentral plass i ny lovgivning. Dersom et lovutvalg for eksempel ønsker å definere «samboer», burde det være lagt til rette for søk etter eksisterende forekomster av ordet, slik at det kunne vurderes om noen av disse helt eller delvis kunne legges til grunn for definisjonen. Uten verktøy og metodikk, er det grunn til å tro at slike søk og analyser bare sjelden vil bli gjort.

Det kan også være mulig å gjøre åpne søke etter definisjoner innen en bestemt systematisk kategori ved å sette systemet opp til å søke etter bestemmelser som inneholder språklige kjennemerker på legaldefinisjoner (f.eks. ordene «legaldefinisjon» og «definisjon» og tekststrenger som «menes i denne lov/forskrift» osv.). Slik oversikt legger til rette for god vertikal og horisontal samordning og sammenheng i lover og forskrifter, men innebærer ikke nødvendigvis at en skal velge samme definisjon dersom en finner et begrep som har nesten likt meningsinnhold som det en ønsker i den nye loven. Poenget er å legge til rette for større grundighet av analyser i utredningsarbeidet og godt grunnlag for begrepsmessige valg, ikke størst mulig grad av samordning.

7 Elektronisk høring av lovforslag

Det er vanskelig å overbevise om nytten av IT-verktøy for lovarbeider bare med ord. Konkrete løsninger i form av prototyper som gjør ting i stedet for å bare beskrive, kan ha eksempelets sterke makt. I LovIT-prosjektet fikk jeg hjelp av vitenskapelig assistent ved SERI, cand jur Odd Kleiva, til å realisere ideer til system for Internett-basert høring av lover og forskrifter. Systemet har separate moduler for høringsinstanser og departementer. Det er ikke her plass til å beskrive mer enn noe av innholdet. Et hovedpoeng er imidlertid at systemet legger vesentlig bedre til rette for departementets analyse og videre bruk

6 Se Dag Wiese Schartum: «Sharing information between government institutions - Some legal challenges» Paper to itAIS2008 http://www.itais2008.org/, Paris, 14. December 2008.

av innkomne uttalelser, sammenlignet med dagens høringer på Regjeringen.no som bare bruker nettsidene som en formidlingskanal.

Ovenfor har jeg klippet ut første siden på modulen som kan brukes av høringsinstansene. Et vesentlig poeng ved denne delen er at det gis full og enkel tilgang til relevant bakgrunnsinformasjon; se horisontal meny. I samme meny er det gjort tilgjengelig funksjoner som legger til rette for at flere personer innen samme organisasjon kan arbeide parallelt med uttalelsen. Den som skal gi innspill til en uttalelse fra sin organisasjon, kan se kollegaenes innspill («Andres kommentarer»), lage egne innspill («Mine kommentarer») og se, eventuelt skrive og redigere direkte i organisasjonens samlede høringsuttalelse («Vår høringsuttalelse»).

Den viktigste nyvinningen i høringssystemet er imidlertid knyttet til den vertikale menyen. Poenget her er at det legges til rette for å strukturere høringssvarene i samsvar med noen generelle problemstillinger og selve strukturen i lovforslaget. De generelle problemstillingene er tenkt å gjelde tverrgående spørsmål vedrørende lovforslaget som helhet. Disse skal kunne spesifiseres på ulike måter, men generelle kommentarer, administrative og økonomiske konsekvenser, lovstruktur og lovspråk må forventes å være aktuelle i de fleste lovsaker (jf. «Gi kommentar til helheten»).

Høringsinstanser kan godt velge *bare* å skrive uttalelse under «Generelt», dvs slik det er vanlig å skrive uttalelser i dag. Det er imidlertid lagt til rette for å kunne skrive spesifikke kommentarer til *hver* av de foreslåtte bestemmelsene. I utsnittet fra høringsrutinen ovenfor, har brukeren valgt å skrive kommentar til § 1-2. Brukeren får samtidig opp lovspeilet for denne bestemmelsen som viser hva § 1-2 er foreslått å erstatte (§ 1). Selve uttalelsen skrives i et fritekstfelt nedenfor (ikke med i utsnittet).

I modulen for departementene utnyttes den nevnte struktureringen av høringsvar ved at systemet sorterer og sammenstiller svar vedrørende samme be-

stemmelse eller emne. Systemet kan også telle og bruke grafiske teknikker for å vise hvilke bestemmelser/emner det er mest/minst kommentarer til. Strukturert angivelse av høringssvar legger også til rette for at departementet lettere og sikrere kan bruke sitater fra høringssvarene i odeltingsproposisjonen.

8 Videre arbeid?

Da LovIT-rapporten ble presentert og systemet for elektronisk høring av lover mv ble demonstrert på et seminar med representanter fra relevante departementer til stede, var responsen meget positiv og innsigelsene så å si fraværende. Etter noen tids tenkepause har Fornyings- og administrasjonsdepartementet og Justis- og politidepartementet gått sammen om å igangsette et prosjekt der en tar sikte på å videreutvikle flere elementer i LovIT-prosjektet. Dette gjelder for det første utarbeidelse og utprøving av et system for elektronisk, Internett-basert høring, med utgangspunkt i den prototypen som er skissert i forrige avsnitt. Parallelt er ambisjonen å utvikle en prototyp av IT-verktøy til hjelp ved utarbeidelse av forskrifter, jf særlig ideene som er nevnt i avsnittene 3 - 6 ovenfor. Dersom piloten er vellykket vil det også være aktuelt å utvikle en slik forskriftsmodul med tanke på utprøving i reelle forskriftsarbeider.

Jeg ser de to departementenes beslutninger om å gå videre med ideene i LovIT-prosjektet som en start på et mer omfattende arbeid som tar sikte på å forbedre kvaliteten av lover og forskrifter. Samtidig kan IT-verktøyene bidra positivt til bedre demokratisk medvirkning i lov- og forskriftsprosessen og - ikke minst - til en effektivisering av arbeidet med å utarbeide regelverk.