

Complex nr. 2/2012

**To arbeider i prosjektet Road to media-aware user-Dependent
self-aDaptive Networks (R2D2)**

Darren Read

NETWORK NEUTRALITY

Dag Wiese Schartum

**RETTSLIGE ASPEKTER VED ANALYSE AV BRUKS-MØNSTRE
KNYTTET TIL DIGITALE TV-SENDINGER**

**DEL AV PROSJEKTET «ROAD TO MEDIA-AWARE USER-DEPENDENT
SELF-ADAPTIVE NETWORKS» (R2D2)**

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

Henvelaelser 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 9788272261411

ISSN 0806-1912

Utgitt i samarbeid med Akademika forlag

Trykk: AIT Oslo AS

Omslagsdesign: Kitty Ensby

Innhold

Network Neutrality	
<i>Darren Read</i>	5
1 Introduction	
1.1 Method	5
1.2 The R2D2 Project	6
2 Network Neutrality	
2.1 What is Network Neutrality?	7
2.2 Deep Packet Inspection (DPI)	11
3 Pros and Cons	
4 Current legal standpoint	
4.1 Privacy	17
4.2 Electronic Communications Law	30
4.3 E-Commerce Law	35
5 Conclusion	
6 Bibliography	

Rettslige aspekter ved analyse av bruksmønstre knyttet til digitale TV-sendinger	
<i>Dag Wiese Schartum</i>	43
1 Bakgrunn	
2 Noen metodiske spørsmål	
3 Noen faktiske og rettslige utgangspunkter for drøftelsen	
3.1 Overordnet beskrivelse av aktører og tjenester	47
3.2 Overblikk over den rettslige reguleringen	49
4 Noen grunnleggende rettsspørsmål	
4.1 Oversikt	52
4.2 Hovedaktører og stedlig virkeområde	52
4.3 «Behandling av personopplysninger»	59

5 Krav til rettslig grunnlag og formålsangivelse	
5.1 Oversikt	75
5.2 Rettslig grunnlag for å behandle trafikkdata	75
5.3 Nærmere om samtykke	79
5.4 Oppsummering	86
6 Spesielt om ivaretagelse av konfidensialitet	
6.1 Oversikt	88
6.2 Grunnleggende plikt til kommunikasjonsvern	89
6.3 Sletting.....	91
6.4 Oppsummering	92
7 Spesielt om innsynsrett og informasjonsplikt	
8 Avsluttende refleksjoner	
9 Litteratur og kilder	
 Tidligere utgitt i Complex-serien.....	101
Bestilling	114

NETWORK NEUTRALITY

Darren Read

1 INTRODUCTION

Network Neutrality is a network design principle which has become the centre of attention in the field of Electronic Communications regulation. This sub-project of R2D2 is tasked with outlining network neutrality and discussing any potential regulations which already go some way to maintaining a neutral Internet. I will be concentrating mainly on the privacy related issues concerning the Network Neutrality debate, but other issues and regulations will also be dealt with. As part of the R2D2 project, the aim is to relate any findings to the media-aware user-dependent self-adaptive networks that are the subject of the main project.

This piece of work will be split into four parts. In Section 2 there will be a short introduction to Network Neutrality. Section 3 will look at the arguments for and against the Network Neutrality principle, attempting to show the arguments from both sides. The final section, Section 4, will look at the extent to which Network Neutrality is supported by the current law; this will concentrate on the European privacy regulations (Data Protection and privacy of electronic communications).

1.1 Method

Researching Network Neutrality has shown up some issues. The most notable being the lack of legal academic work on point, this is especially the case regarding academic work, in the English language, emanating from Europe. What literature there is out there is mainly from the US where the Network Neutrality debate is far louder than it is currently this side of the Atlantic. Therefore, I have had to use research methods conducive to this situation.

Sections 1 and 2 are based on a study of the literature that does exist. These sections do have a slight bias to American sources and does highlight the state of the debate in the US. This is down to the situation as stated above. This, however, doesn't affect the applicability of the piece to the European based R2D2 project as the principle is the same throughout the world; it is just the possible regulations which are different.

Section 4, which deals with the regulation of Network Neutrality, is obviously based in the European context. Due to time restraints the project has concentrated on the legislation emanating directly from the European Union, rather than how that legislation has been applied in the member states. This provides an indicative viewpoint on the desired ends of the legislation, but it is important to note that there may be differences between the application of the EU legislation in the member states. This section has had to rely heavily on the text of the directives and reports coming from the EU rather than academic literature as, as noted above, there is very little of this coming from Europe. Where such literature does exist I have made as full a use of it as possible.

Throughout the piece I will be referring to R2D2 networks and to the R2D2 project. To gain a fuller insight into the actual issues regarding these networks I have conducted some informal interviews with other project members.

1.2 The R2D2 Project

The R2D2 project, to which this subproject is part of, is looking at the media-aware user-dependent self-adaptive networks in the provision of content over the Internet. It looks at networking methods of providing Quality of Experience (QoE) over the Internet by improving the Quality of Service (QoS). In short, the project is looking at ways that content providers can provide that content to its users in a better way considering the current architecture of the Internet. Network Neutrality concerns are relevant here as methods of improving the QoS to improve the QoE is through prioritising preferred content which potentially goes against the Network Neutrality principle.

2 NETWORK NEUTRALITY

2.1 What is Network Neutrality?

The current Internet is neutral, in the sense that there is no discrimination between legal content¹ available to all end users (bandwidth and geographical constraints aside). A user accessing the Internet with Telenor as their ISP in Norway can access the same range of websites and view generally the same range of content as a user in the UK who gain access through BT. There are some exceptions to this, for example, some content is only viewable in certain geographical areas due to copyright and licensing restrictions. Other content is filtered out by ISPs due to its illegal nature, for example child pornography. However, “there is no way that the Net has to be; no single architecture that defines the nature of the Net.”²

First and foremost Network Neutrality is a network design principle. However, more recently it has begun to take on aspects of law, politics, economics and sociology. This has lead to it being discussed as a legal principle, however, when in the legal and political field it is still at the stage of being more an aim, something which is part of policy, but yet to be enshrined in law.³ The term “Network Neutrality” is fairly recent, having been coined by Tim Wu in 2003.⁴ However the main concepts of the principle existed through other design principles upon which the Internet was based. The end to end (e2e) principle requires that the intelligence in a network is concentrated at the edge of it. The actual network itself should be dumb, this is the total antithesis of the older telephone networks where the network is “smart” and the ends (the telephone) are “dumb”. The Internet was originally built with e2e in mind. The network that carries the communications between end points originally

1 Legal content as opposed to content prohibited by law. This can be hard to ascertain considering the global nature of the Internet and the different laws in different countries. A further discussion is not warranted here, but suffice to say some things are almost universally prohibited around the world due to international agreements, for instance copyright infringement and the viewing of child pornography.

2 L Lessig, *Code v2*, (New York: Basic Books, 2006) at pg 32.

3 However, in some places, most notable The Netherlands and Chile, it has been enshrined in law already.

4 T Wu, “Network Neutrality, Broadband Discrimination” *Journal of Communications and High Technology Law*, 2: 141 (2003) available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=388863.

just transported the packets of data from one end to the other; it did not do anything else. A network that follows the e2e principle is necessarily a neutral network as there will be no means of the network discriminating between data packets.

Due to Network Neutrality transcending boundaries between network design, law, politics, economics, and sociology, it is hard to define totally and completely in a single definition. There have been a number of attempts but these vary subtly from one another over both scope and wording. The best definitions have generally come from governmental sources and academics, sources from those involved directly with the provision of Internet services or content tend to define Network Neutrality in a way that best suits them, so these should not be generally viewed as authoritative. In a US Congressional Report the Congressional Research Service wrote:

Most agree that any such definition should include the general principles that owners of the networks that compose and provide access to the Internet should not control how consumers lawfully use that network; and should not be able to discriminate against content provider access to that network.⁵

Whilst in the UK the telecommunications regulator Ofcom has defined the outer limits of the principle as:

The purest version of 'net neutrality' assumes that:

- *There should be no prioritisation of any type of traffic by network operators; and*
- *Those providing content, applications and services via the open Internet should not be charged by network operators/ISPs for the distribution of that content to the network operator/ISPs' customer base⁶*

The Federal Communications Commission (FCC), the US telecommunications regulator, has set out four elements on Network Neutrality. These were released in a policy statement so were intended to act as a form of guideline to ISPs over what behaviour is expected. However, following the Comcast decision (which I come back to later) the courts have made it clear that the FCC has no legitimate basis to enforce these. So, in practice, these four elements merely act

5 CRS Report for Congress, Net Neutrality: Background and Issues, 2008, available at: www.fas.org/sgp/crs/misc/RS22444.pdf.

6 Ofcom, traffic Management and 'Net neutrality', 2010, available at: <http://stakeholders.ofcom.org.uk/consultations/net-neutrality/>.

as a further definition of what the FCC believes Network Neutrality to be. The four elements are that consumers are entitled to:

1. *Access the lawful content of their choice.*
2. *Run applications and use service of their choice, subject to the needs of law enforcement*
3. *Connect their choice of legal devices that do not harm the network*
4. *Competition among network providers, application and service providers, and content providers.*⁷

Finally, from an academic standpoint, Tim Wu suggests that “a maximally useful public information network aspires to treat all content, sites, and platforms equally.”⁸ Going further than most, Christopher Marsden considers Network Neutrality as two distinct sub-principles. “Positive” Network Neutrality looks at the prospect of charging more for better access, for instance on Next Generation Networks (NGNs). “Negative” Network Neutrality concerns throttling, degrading or blocking users’ access to Internet content. This can be summarised as “charging more for more and charging the same for less”.⁹ Marsden suggests that it is just the negative backward facing element that should be restricted.¹⁰

These definitions all agree on one thing; that the blocking of content is in violation of Network Neutrality. However, beyond that there are unassailable disagreements between them. The definitions emanating from US governmental sources (Congress and the FCC) specify that Network Neutrality extends only to legal content, this will obviously lead to rather large loopholes for ISPs to exploit as “legal” can be open to interpretation. Including legality of content in the definition could allow ISPs to block, for instance, all P2P traffic due to it being apparently mainly used for copyright infringement. The other differences are best described using Marsden’s classification of positive and negative Network Neutrality. The Congressional Report and Ofcom definitions both go on to prohibit any discrimination of Internet traffic at all, regardless of whether this is done on a non-price-discriminatory basis. This accords with both the negative and positive aspects as defined by Marsden. However,

7 FCC Principles, available at www.publicknowledge.org/pdf/FCC-05-151A1.pdf. The FCC has made another attempt at regulating Network Neutrality through a Report and Order released on 23rd September 2011, the result of which has yet to become fully apparent. “Preserving the Open Internet; Report and Order; FCC” 76 Federal Register 185 (23rd September 2011) p 59192 – 59235.

8 http://timwu.org/network_neutrality.html.

9 C Marsden, *Net Neutrality* (Bloomsbury, 2010). Kindle edition: (A&C Black, 2010) at 1116 (Kindle Ref).

10 Marsden *ibid*.

the FCC and Tim Wu concentrate on the provision of competition and non-discrimination between similar content providers. This allows for prioritising some traffic as long as this is done on a non-discriminatory basis, that the same terms are offered to all content providers. This will usually be offering the same price to all content providers who wish to reach customers on the ISP's network.

These two definitions are impossible to consolidate into one catch all definition. Therefore throughout this piece I will use Marsden's two part definition as the basis for the discussion on network Neutrality. Negative violations of Network Neutrality shall mean blocking access to certain content, or degrading or throttling specific content for any purpose. Positive violations of network Neutrality shall mean any non-discriminatory prioritising of certain Internet traffic. Although this will inevitably leave less bandwidth for all non-prioritised traffic, that restricted bandwidth will have no discrimination on it and all non-prioritised traffic will be treated equally. R2D2 networks which use prioritisation as a means to providing improved QoE are mainly concerned with the positive aspects of Network Neutrality. That is providing over the top prioritised services to the end user. Therefore, they go against the design principle as enunciated by the Congressional report and Ofcom, but would be acceptable following the FCC and Tim Wu's work.

In accordance with the definitions which will be used throughout this piece, I will take the situation where ISPs have totally autonomy and freedom to do as they will with regards to discriminating between content as my point of departure. As Network Neutrality is a design principle and not a legal principle in its own right there is no general legal rule saying that they cannot do as they will. So, with total ISP autonomy and freedom as the presumption I will look at the various legal rules on point which exist as restricting this ISP freedom with regard to Network Neutrality. The areas of law that will be looked at are data protection and privacy, electronic communications regulation, and e-commerce law.

It is necessary here to distinguish between traffic management for the smooth running of the network, and traffic management for economic gain. The Internet is getting busier and busier, there is a finite capacity and at times, especially in bottlenecks such as the ISPs' networks going to the customers, they can become clogged. In these situations the network operator will have to perform some traffic management to keep the network running. This, most people agree, is a perfectly acceptable practice as long as the choices made in managing the traffic are non-discriminatory. That is that the network routers don't drop packets from low value customers or from certain content providers, but delay all traffic the same. The other form of traffic management is that for economic gain through discriminatory or non-competitive behaviour.

.....

This is where traffic management is not neutral, where packets are differentiated by content, sender, or receiver, generally for added economic gain by the network provider. Even though reasonable traffic management has an economic gain for the operator in terms of a smoothly running network is a more valuable network, the economic gains referred to in the discriminatory system are those above and beyond the economics of running a network. The economic gain can come from activities which are either against the negative or positive aspect of Network Neutrality. Relating this back to R2D2 networks, the added economic benefit here would be a guaranteed service for providing high bandwidth content; something that is likely to be very attractive to consumers.

2.2 Deep Packet Inspection (DPI)

Before I go into the advantages and disadvantages of a neutral Internet it is important to introduce the technology behind any potential discrimination of Internet content. The group of possible filtering methods are known as Deep Packet Inspection (DPI). This is not just one technology, but the general term for a number of different techniques which categorise data type and actual content. The alternative, Shallow Packet Inspection (SPI, or just packet inspection),¹¹ is only capable of looking at information required to route the packet to its destination, this is only appropriate for the blocking of communications by port number.¹²

When ISPs have decided that they wish to discriminate between some types of content for whatever reason¹³ they must first have knowledge of what sort of data the packet contains. The most likely form of discrimination to take place will be either on data type: for instance whether a packet is associated with a P2P file sharing application or WWW traffic; or whether the sender (content provider) has an agreement in place for better service. The data for this type of discrimination is not self-evident from the packet header; data used for the routing of the packet only, and is thus not ascertainable using SPI only. So, for ISPs to gain knowledge of what type of data a packet contains in order to decide whether to favour or discriminate against it they must look deeper into the packet to enable them to correctly categorise it, hence the name deep packet inspection.

11 For more information see http://www.Thetanetworks.com/resources/shallow_packet_inspection.html.

12 Which is susceptible to spoofing, this is discussed later.

13 These will be discussed further below.

The use of DPI is controversial due to its ability to “essentially eliminate online privacy as it exists today”.¹⁴ When an ISP utilises DPI technology to categorise traffic on its network it potentially has the ability to monitor and catalogue all of its end-users’ communications:

*it is possible to tell whether a packet stream is VOIP, email, web browsing, instant messaging, video streaming, file transfer, or peer to peer file sharing. It is possible to examine in detail the content of the email, or web page, or downloaded file. It is possible to distinguish music files from text from pictures. It is possible to search for keywords within any text.*¹⁵

DPI is required regardless of whether the Network Neutrality involved is positive or negative by Marsden’s categorisation.

DPI works by recognising the signature that a certain application makes when it is travelling over the Internet. A DPI system creates and stores signatures for different types of traffic and then compares any communications’ signatures with the resulting database, thus identifying what application is being used. This signature creation process can take a number of forms,¹⁶ for instance, the simplest method constitutes SPI and is analysing the port that the packet is using. However it is relatively easy to use non-standard ports for certain applications so that a router cannot identify it, for instance some P2P file sharing applications have been known to use port 80, the port commonly associated with web browsing.¹⁷ Other methods include looking at the sizes of packets; larger packets tend to mean that it is file sharing of some description. The most advanced method of DPI involves tracking the behaviour of packets in very fine detail. This includes looking at size of packets, the header information, and any responses which may result from it. Different applications will have a different response to receiving a packet and this can be detected and used to categorise the traffic type. Finally, some techniques involve looking at the actual content inside the packet. This is a very useful technique for both surveillance by security services and behavioural advertisers. For instance, the much maligned Phorm advertising system which is

14 Alissa Cooper, The Singular Challenges of ISP Use of Deep Packet Inspection, 2010, available at <http://www.deeppacketinspection.ca/the-singular-challenges-of-isp-use-of-deep-packet-inspection/#more-68>.

15 Jon M. Peha, The Benefits and Risks of Mandating Network Neutrality, and the Quest for a Balanced Policy, International Journal of Communication, Vol. 1, pp. 644-668, 2007.

16 See e.g. Allott Communications, Digging Deeper into Deep Packet Inspection, 2007, available at <https://www.dpacket.org/articles/digging-deeper-deep-packet-inspection-dpi>.

17 Jerome Tollet, Myth 3: Applications Respect Well Known IANA Ports, 2008, available at <https://www.dpacket.org/articles/myth-3-applications-respect-well-known-iana-ports>.

based on detailed user traffic surveillance to create hugely detailed user profiles is based on DPI technology.¹⁸ This system is currently under investigation by the European Commission¹⁹ with respect to Data Protection regulations and communications surveillance rules, both of which I will come back to later. DPI is the primary method used by police and intelligence services to monitor communications over the Internet. For instance in the US the NSA has utilised it to create a comprehensive monitoring policy over international communications to and from the US. The privacy concerns which this can cause will be discussed in section 4.1 which looks at issues revolving round data protection law and privacy of communications.

18 <http://www.phorm.com/>.

19 Commission launches case against UK over privacy and personal data protection at <http://europa.eu/rapid/pressReleasesAction.do?reference=IP/09/570>.

3 PROS AND CONS

There are different viewpoints on how desirable the network neutrality principle is. On the one hand there are those who support enshrining Network Neutrality in some form of regulation and view it as a cornerstone of the current Internet and required for further innovation. Some of the most important academic proponents of network neutrality are Tim Wu,²⁰ Lawrence Lessig²¹ and Yochai Benkler.²² The fear is that if ISPs and access providers no longer treated traffic from all content providers equally they could start discriminating against certain content or applications for a number of reasons. They could discriminate against high bandwidth applications such as P2P file sharing to enable the network as a whole to function better. However, they could also start charging content providers for access to their customers and block or degrade the connections to others. The worst case scenario is the balkanisation of the Internet with some websites only being available through some ISPs; this would create walled gardens of content and restrict end user choice dramatically.²³ For example Amazon could do an exclusive deal with ISP A to ensure it is the only book seller available to ISP A's customers, or ISP B could degrade the traffic speed to all search engines other than Google if Google pays them more money for access to their network and customers. This is the very worst case scenario; a more realistic approach might be for an ISP to favour its own content over other content providers. This is becoming more and more of a risk due to the vertical integration and consolidation of content providers and access providers. In this scenario ISP C could have its own video streaming service and could either speed up the access to this service or degrade the access to competing services such as YouTube.²⁴

Another worry would be the pace of innovation. At the moment, with a neutral Internet, anyone can create a website or service on the Internet and it is automatically available to everyone with relatively small start up costs (for distribution). If ISPs were to start charging everyone for access to their customers the barriers for market entry would suddenly be huge. It would be hard

20 See no. 8 above.

21 See e.g. *Code v2*, (New York: Basic Books, 2006); *Future of Ideas*, (New York: Random House, 2001).

22 See no. 1 above.

23 J Stanley for the American Civil Liberties Union (ACLU), "Network Neutrality 101: Why the Government Must Act to Preserve the Free and Open Internet", October 2010, available at http://www.aclu.org/files/assets/NetworkNeutrality_report_20101019.pdf.

24 Marsden (2010) at 1147.

enough to pay for access to ISPs in one country, but to be required to do it for ISPs throughout the world would be prohibitively expensive and confusing.²⁵ So the fertile conditions which lead to Facebook, Google, or Skype would be far more barren.²⁶

On the other hand, it can be argued that not allowing ISPs and access providers to discriminate will lead to more and more congestion on the Internet. More and more rich content is becoming available and this has the potential to clog the pipes of the Internet and bring it to a standstill. To enable ISPs to charge content providers, content providers who some ISPs accuse of “free riding”,²⁷ would lead to much needed funds and incentives to upgrade the infrastructure, thus providing more bandwidth. An alternative, or in addition, to charging content providers there is also the possibility of allowing consumers to purchase a guaranteed faster service. This would replace the best effort service currently available with a guaranteed bandwidth which would be attractive to those users who access high bandwidth services such as HD video, gaming, or Voice over IP (Internet telephony, such as Skype). These services are more susceptible to delay, unlike email or normal web browsing. However, the neutrality proponents would argue that this would provide a disincentive to the ISPs as it would be in their best interests to keep the basic service reasonably slow to entice people to buy the “premium” service. If they invested enough in infrastructure to make the basic package useable for all but the most bandwidth hungry applications then there would be no reason for all but the heaviest users to pay the extra for a faster service.

Currently the threats which I have briefly described above are only perceived threats. There is, as yet, no evidence of any widespread systematic throttling, degrading, or blocking of access to services. There has been no systematic breaching of the Network Neutrality principle, either negatively or positively. However there have been two US cases on point which has lead to the perceived threat becoming more real with the FCC being declared impotent with regard to regulating Network Neutrality under its current authority. In the Madison River case²⁸ the ISP, Madison River, was blocking access to VoIP services provided by another company. This was settled out of court, but it was the first time the FCC had shown willing to enforce Network Neutrality. The most important case, however, is *FCC v Comcast*.²⁹ Here the ISP was blocking

25 Over time the problem of signing agreements with all ISPs might disappear with a service for registering with all ISPs for a certain one off (probably still large) cost.

26 ACLU (2010).

27 See e.g. At&T's, Ed Whitacre's comments to the Business Week magazine in 2005, quoted in Marsden at 1107 (Kindle).

28 See http://hraunfoss.fcc.gov/edocs_public/attachmatch/DA-05-543A2.pdf.

29 See http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-08-183A1.pdf.

P2P file sharing applications. Again the FCC decided to act and try to enforce its Network Neutrality principles through the courts. This went to court, but the FCC lost on grounds that it had no basis for regulating ISPs in such a way. The Comcast decision is regarded as something of a watershed moment with the New York Times suggesting that it could allow “Internet service companies to block or slow specific sites and charge video sites like YouTube to deliver their content faster to users.”³⁰ It is this that has led to the emergence of Network Neutrality as a mainstream issue, no longer just a theoretical problem without any real relevance. To my knowledge there have been no court cases concerning Network Neutrality in Europe.

Following the Comcast decision the FCC has been holding a series of confidential meetings with the largest companies on both sides concerned with Network Neutrality.³¹ These broke down towards the end of July 2010. Following these talks Google and Verizon, a large US Internet Access provider, released a joint paper with their views on what should be done to maintain Network Neutrality. This document suggests that Network Neutrality should be enshrined in law, to an extent. It provides two, rather large, exceptions. The first being an undefined group of services called “additional online services” which are just other services which could cover most new applications over the Internet. The second being wireless broadband connections. These two areas discrimination would be allowed.³²

30 “U.S. Court Curbs F.C.C. Authority on Web Traffic”, New York Times, April 6th 2010, available at http://www.nytimes.com/2010/04/07/technology/07net.html?_r=1.

31 “Transparent’ FCC Continues Secret Meetings”, *Daily Finance*, June 22nd 2010, available at <http://www.dailyfinance.com/story/company-news/public-interest-groups-appalled-by-closed-door-fcc-web-meeting/19527046/>.

32 See the Google Policy Blog, August 9th 2010 at <http://googlepublicpolicy.blogspot.com/2010/08/joint-policy-proposal-for-open-internet.html>.

4 CURRENT LEGAL STANDPOINT

4.1 Privacy

4.1.1 Data Protection

There are some obvious privacy concerns relating to DPI and thus to the potential discrimination of Internet traffic. These can be split into two main areas which I will discuss in turn. Firstly there are concerns relating to data protection, that is informational privacy concerns about data collection, processing and usage. The second area I will look at is privacy of communications.

The European data protection regulations are amongst the toughest in the world and the collection and processing of personal data is heavily restricted. The following discussion will relate directly to the contents of the European Directives on point. Although these are not directly applicable to national law they give well founded expectations of the main structure of the laws of the nation states. The aim and outcomes of a directive must be incorporated into national law, but there is some flexibility over exactly how this is done.³³

To discern how relevant to Network Neutrality the EU data protection regime is it is first necessary to discuss the basics. For the Data Protection Directive (DPD)³⁴ to be relevant there needs to be the processing of personal data. As I have discussed above, the data which is being processed when DPI technologies are utilised is both traffic data and content data of the Internet communications. This could potentially involve ISPs building up a record of the history of natural persons web browsing and their use of any other Internet services (such as VoIP or P2P file sharing). Personal data is defined by Article 2(a) of the Data Protection Directive and is “any information relating to an identified or identifiable natural person ...; an identifiable person is one who can be identified directly or indirectly...”. When identification is done indirectly it must be “likely reasonable”³⁵ that such identification will happen with the use of other data available to the data controller.³⁶ There are two types of

33 For a full discussion of the Norwegian Data Protection regime I refer to Dag Wiese Schartum's paper on point relating to the R2D2 project printed in this book.

34 Directive 95/46/EC on the Protection of Individuals with Regard to the processing of Personal Data and on the Movement of such Data.

35 Recital 26 Data Protection Directive.

36 “Data Controller” is defined by Art 2(d) of the DPD as a natural or legal person who “determines the purposes and means of the processing of personal data”.

data which may be captured by the monitoring systems required for packet discrimination.

Firstly there is the traffic data. This is the data concerning the IP addresses and port numbers related to the packets of data monitored. Depending on where on the route from sender to recipient surveillance takes place, this may or may not be classified as personal data in itself. There is also the possibility to flag certain packets as prioritised in this packet header. Take the situation where User A is viewing a video on YouTube. User A's ISP will be able to associate the IP address that it sees on a packet as belonging to User A as they have allocated him that IP address, they have that additional information so will be able to identify him indirectly, but quite easily. Therefore the IP address here is personal data in itself. If the surveillance happens upstream of the users' own ISP then associating an individual, or group of individuals, (in the case of a household Internet account) will be much harder as the data on who has which IP address assigned to them at a certain point in time won't be readily available. If this is the case then the chances of it being associate with an identified data subject will not be "likely reasonable".

However, in certain circumstances it has been shown to be possible to identify individual users simply from search terms input into Internet search engines. For instance, a 62 year old Georgian widow called Thelma Arnold was identified by The New York Times following the release of supposedly anonymised search data by AOL.³⁷ Each user was given a unique ID, and from the searches done by user 4417749 it was possible to identify who that person was. With a list of websites that a specific IP address visits it may be possible to identify the individual who was using that IP address at the time. However, given that in the AOL case the process was very labour intensive and took a lot of time, and the likelihood that one person will only have one IP address at a time being low, it is not likely reasonable that someone from an upstream ISP would go to the effort to identify individual users in this way and thus traffic data here will not be classified as personal data and the Data Protection Directive will not apply.

So, in summary, the traffic data associated with the Internet communication is likely to be classified as personal data when it is processed by the users' own ISP due to the relative ease in which the user can be identified from it. However, an upstream network operator, for example a tier 1 backbone operator, would not be likely reasonable to identify the user from traffic data alone as they do not easily have access to further data to identify the user.

37 "A Face Is Exposed for AOL Searcher No. 4417749", *The New York Times*, August 9th 2006, available at <http://select.nytimes.com/gst/abstract.html?res=F10612FC345B0C7A8CDDA10894DE404482>.

I will now move on to the actual contents of the Internet communication. When DPI is used the amount of data which the ISP monitors will vary, but the potential is there for them to monitor everything that is contained within the packet.³⁸ To what extent they have the motivation to do such monitoring is, however, slightly more questionable. To instigate a regime of monitoring to enable discrimination of Internet traffic not all aspects of the data contained is necessarily required. For instance if the ISP is using the behaviour³⁹ of the packets as their basis for determining if it is P2P, WWW, etc. then there is no need to look at the contents of the communication in detail. That it behaves like an email is enough to determine that it is an email without looking at the text of the email itself. The amount of data that an ISP collects is important over whether it is classified as personal data. As stated above, traffic data alone constitutes personal data for the users' own ISP, so delving deeper into the packet makes no difference with the decision for contents. However, depending on the depth, the monitoring of content data using DPI may be classified as processing personal data for upstream ISPs. This will depend on the depth that the inspection takes, but it would seem clear that if the upstream ISP is looking at the actual contents (text of an email, etc.) then this would be personal data and be within the scope of the DPD, as will any data collected which relates to email addresses, postal addresses or, most definitely, names. Behavioural monitoring is less clear cut, without access to the actual contents or who the IP address is associated with, it will still be very difficult for an upstream ISP to identify the user.

Beyond the normal category of personal data Article 8 of the DPD sets out "special categories of data"⁴⁰ which have a tougher set of rules relating to their processing. These special categories of data are data which reveals: "racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life". When being processed by the user's ISP, the combination of the traffic data (identifying the individual) and content data, could sum up to this sensitive data. Again, depending on how deep the monitoring goes, any website which a user visits could give away certain facts about themselves. For instance they could be looking up a certain political party's website or searching for information relating to a disease. Although this is not proof that the user is a follower of that certain political party or that they have that disease, it could be a strong indication which can become stronger over time depending on the future browsing. Obviously, more detailed profiling of a user could result

38 Peha, no. 15 above.

39 Allott Communications, no. 16 above.

40 Also referred to as sensitive data in recitals 34 and 80.

in there being no doubt as to the sensitivity of the data. A user being able to login using a personal username and password to certain websites would be very strong proof of an affiliation to that websites content or views. Without the user being identified by the traffic data, as is the case with other network operators other than the user's which transits the communication, the same problems persist here as with normal personal data. However, where the data is identifiable and relates to one of the above classes (racial or ethnic origin etc) then it will be sensitive data also.

Finally there needs to be some form of processing of this personal data. Article 2(b) of the DPD defines processing as: "collection, recording, organisation, storage, adaptation or alteration, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction." Using the personal data (if it is classified as such) as the basis for discrimination of Internet traffic would constitute processing of the data. It would satisfy "collection", "consultation" and "use" and depending on what is done after the discrimination process has taken place, possibly "recording" and "storage".

When a network operator manages traffic without discrimination, normally to keep the network running smoothly during times on congestion, there need not be any DPI. Packets can be delayed without prioritisation, and as such, there need be no further inspection of packets other than the normal routing protocols.

When these rules are related to R2D2 networks, there is the potential for there to be some processing of personal data, however, the extent to which this is the case can be limited. If a network can work efficiently enough using just flags and IP addresses then the amount of personal data being processed is kept relatively low, for example the user's IP address. If, however, prioritisation is done solely on the content provider's IP address then there will be no processing of personal data at all (the DPD only relates to natural persons).⁴¹ In the circumstance where a content provider has an agreement with the user's ISP that content coming from IP address 123.123.123.123 shall be prioritised but content coming from IP address 234.234.234.234 will not then the user's IP address will not be processed above and beyond the normal routing protocols. The same will be the case if flags are used, whether on their own, or in conjunction with the content provider's ISP address. If this is the case then there will be no privacy concerns as there is no way of identifying the user who is accessing the content, in this case the DPD will not come into play. As there is some potential for the processing of personal data in R2D2 networks I will now look at when such processing can be allowed.

41 Article 2(a) DPD.

If a certain set of data has been classified as personal there are then restrictions on whether it can be processed or not. The DPD splits these restrictions into two aspects, first there are principles relating to the data processed itself (as set out in Article 6) and then there are legitimate reasons for processing any personal data (article 7), I will discuss the two in turn.

Article 6 of the Directive lays down principles relating to the data that is processed. The most pertinent here are 6(b) and 6(c). Article 6(b) states that “data must be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes”. Collecting the data for means of discrimination and prioritisation may well be a legitimate purpose if it is explicitly specified as such. However, where the equipment is installed for one purpose, for behavioural advertising for instance, the data collected for that purpose cannot then be used for traffic management and discrimination without that other purpose being specified explicitly also. The same would be for data collected for national security, or, indeed, any other reason not contiguous with discrimination. That data could not legally used for discrimination without disclosure of that fact.

Article 6(c) states that the data must be “adequate, relevant, and not excessive in relation to the purposes for which they are collected/further processed”. Firstly, it must be ascertained whether the personal data which is necessarily processed when using either DPI is adequate and relevant for discriminating against content on the Internet. The data used, such as IP addresses and any content which may be monitored, is necessary for DPI to work. Therefore it is clear that some of the data which is processed is adequate and relevant for the task at hand. However, in some cases, depending on the DPI techniques being employed, there may be some irrelevant data collected. ISPs and network operators, therefore, must be careful to only monitor to the depth that they need for their particular discrimination requirements and not collect extra data, such as the actual text of an email, when it is not strictly required for the discrimination process. These extra data would then be irrelevant to the purpose for which they are processed. So, as long as ISPs are careful not to collect data just for the sake of it then the data processed should be considered adequate and relevant. However, for it to be considered as not excessive it must be a necessary technique for implementing such discrimination regimes. Here we must use the least drastic means test: “it must be established whether the measure is necessary to achieve that aim, namely, whether there are less restrictive means capable of producing the same result”.⁴² A less drastic means than DPI would be Shallow Packet Investigation, as noted above this only looks at traffic information such as IP addresses and port numbers. This can involve the

42 T Tridimas, *The General Principles of EC Law* (Oxford: OUP, 1999).

processing of personal data (IP addresses) or not (port number), but it is less privacy invasive than monitoring the contents, therefore is a less drastic means of achieving the end aimed for. However, as Marsden has stated, this technique will not be effective in categorising content for discrimination at all times as it is a relatively simple process to use non standard port numbers such as disguising P2P as WWW content using port 80. Therefore DPI would appear to be the least drastic means (but still quite a drastic means) of achieving the end of categorising packets to enable discrimination. Therefore, using DPI as a means for discrimination of Internet traffic will fulfil Article 6 of the Directive as long as certain precautions are taken. These being, firstly that the data be collected directly for discrimination, or if not it must be disclosed that the data collected for some other purpose will be further used for discrimination. And secondly, there must not be more data processed than is strictly necessary for the aim of successfully categorising Internet traffic for discrimination. As stated above, R2D2 networks may not need to utilise DPI techniques if IP addresses and flags can suffice. But if such over the top services become popular with consumers there is likely to be some attempts to get prioritised service without paying for it. Companies might fake flags on their packets or copy a privileged IP address. Then using non-personal data will not be sufficient and DPI techniques may be required to make the system work correctly. In this arms war scenario the least drastic means would slowly ramp up in correlation with the sophistication of parties who scam the system.

The data processing operation also has to fulfil Article 7 of the Directive. This lays down several specified situations where processing will be allowed, the presumption being that processing will not be allowed unless at least one of these is fulfilled. The most relevant of these are (a), (b), (e) and (f).

Article 7(a) states that processing can only take place when the data subject has given their “unambiguous” consent to the processing. Article 7(b) runs along similar lines in that processing can take place if it is necessary for the performance of a contract. In the case of the relationship between ISPs and their customers, any consent will be in the form of a contract setting out the user’s consent to the processing of their personal data, so these can both be taken together.

If the data is judged as coming under a “special category of data” as defined by Article 8(1), as discussed above, then the processing of these data is even stricter. There are five reasons why such data can be processed, the only relevant one being 8(2)(a) which requires “explicit” consent from the data subject. This goes further than “unambiguous” consent as required for the processing of normal personal data under Article 7(a). If the data are classed as falling into one of these special categories then the legitimate reasons under Article 7 no longer apply, so the only valid reason for processing these data

for discrimination of Internet content, pursuant to the DPD, would be 8(2)(a), namely explicit consent.⁴³

Consent is defined by Article 2(h) of the Data Protection Directive, and states that consent must be “freely given specific and informed indication of his wishes... to personal data being processed.” Various factors must be taken into account when deciding whether an indication of consent can satisfy those criteria. For consent to be informed there must be sufficient notice of the processing that is going to take place.⁴⁴ In the case of ISP discrimination of Internet traffic this would have to lay out the data which will be monitored by the ISP when using their particular DPI system. Freely given consent means that there must be no coercion to agree to a certain processing operation. This implies that there must be real alternatives to the data subject which won’t see them incur penalties.⁴⁵ However, as Bygrave and Schartum put it:

*The degree of choice presupposed by these mechanisms will often not be present for certain services or products, particularly those offered by data controllers in a monopoly (or near-monopoly) position.*⁴⁶

The level of competition in the ISP market differs between jurisdictions. However, for a market such as that in the US, where the vast majority of home users have to choose of just two providers, there clearly isn’t the choice of ISP to be able to give consent freely. European markets are generally more competitive, but in some rural areas the choice afforded to the user will be severely limited. Given the (ever growing) importance of an Internet connection in the modern world the choice between Internet that processes vast amounts of personal data and no Internet connection is not an equal choice. The user will definitely be at a severe disadvantage if they choose not to allow personal data processing in such a situation. Where there is more competition consent may be able to be freely given depending on the choices available. However if monitoring becomes the norm and all ISPs utilise the same DPI technology then the choice afforded to the users will once more be non-existent.

43 Article 8(2)(a) Data Protection Directive.

44 A list of information which must be communicated to the data subject is contained in Articles 10 and 11 of the Data Protection Directive and include information such as the identity of the data controller and the purpose of the data processing operation.

45 This aspect of consent is used by the Norwegian Post- og teletilsynet’s (NPT) Guidelines on Network Neutrality, which will be discussed below.

46 L.A. Bygrave and D.W. Schartum, “Consent Proportionality and Collective Power” in S Gutwirth et al (eds), *Reinventing Data Protection?* (Heidelberg: Springer, 2009) pg 157–175 at 160.

Where monitoring is done by an access provider other than the users ISP (for instance a tier 1 backbone provider) then there will be no direct relationship between user and provider and thus consent will not be evident. It can be argued that there would be some form of implied consent by users as they know that their Internet traffic will be transited by a number of other networks, even if there is no way of predicting which networks exactly. However, implied consent cannot constitute a valid consent under the DPD. Even if implied consent could constitute consent this is not a valid argument, as the user has no choice regarding the route their data takes across the Internet. They cannot specify a route which doesn't have any monitoring technology installed. Here the choice would again have to be Internet connection or no Internet connection, which is not a valid choice for the user to make. Further to that, as I have stressed above, some data will be sensitive personal data, and this requires the higher standard of explicit consent. Given that the user will not know over which networks their communications will travel it is impossible for them to give their explicit consent to the processing of that data. Therefore, due to the existence of some sensitive data amongst Internet traffic, consent cannot be given for categorising data for discrimination of any kind when done by a network other than the user's ISP en route from sender to receiver. Consent can only be a justification for processing personal data when it is conducted by the user's ISP.⁴⁷

If a user has paid for prioritised service, as would be the case when accessing over the top services on an R2D2 network, then this should be considered as them consenting to that service. If there is full disclosure by either the content provider, or more likely the user's ISP, then this will be entirely sufficient to allow the data processing to take place. If however, the processing that might take place (again this is presuming that personal data processing is required for R2D2 networks) is not explained to the user then consent is not informed and thus not valid. When we are talking about content there is less of an argument that the choice between accessing the content and not accessing the content is not a real choice. There are always going to be some services which people aren't going to access either due to cost or privacy concerns, but these are by no means as fundamental to society as an Internet connection. This assumption can, however, be tempered depending on the content on offer. Public broadcasters (NRK, the BBC) are in a different situation to private entities and such content providers will likely have to provide the same range of content to users without any prioritisation as well if they decide to offer prioritised services.

47 P Ohm, "The Rise and Fall of Invasive ISP Surveillance", *University of Illinois Law Review* 2009, available at <http://ssrn.com/abstract=1261344> at pg 63-65.

Article 7(e) provides for processing where it is “necessary for the performance of a task carried out in the public interest...”. For this to be valid grounds for processing the smooth running of the telecommunications network would have to be considered as in the public interest. Even if that were the case this would only prove a valid grounds when the data was processed to make the network run smoothly (traffic management) not when the processing is for the economic interests of the controller (discrimination). This further discrimination would be considered a secondary purpose to the primary intention of a smooth running network and thus the data could not be processed for discrimination in accordance with the specification principle in Article 6(b).

Article 7(f) states that:

Personal data may be processed only if processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1(1). (emphasis added)

This catch all clause introduces a balancing exercise between the interests of the controller and the rights of the user. In the case of network discrimination, ISPs have a legitimate interest in processing the data for traffic management. However this interest must be deemed greater than the users’ fundamental right to “privacy with respect to the processing of personal data”.⁴⁸ The balancing test would have to take into account the degree to which the technology involved interferes with the user’s privacy. As I have stated earlier, there are different methods of categorising packets for discrimination. From the literature on DPI there seems to be a correlation between privacy invasiveness and effectiveness of the technology. For instance the least privacy invasive method of categorising packets is looking at the port number. This port number is not privacy invasive in itself as it is simply a number relating to application that is being used. However, this isn’t a very effective method as spoofing of port numbers is relatively easy. The most privacy invasive method is a very deep monitoring of the contents of the packet to determine what kind of data it is. This also happens to be the most effective form of discriminating which can only be beaten with the use of encryption tools. So the privacy concerns of the users fall on a continuum between the two extremes and this then has to be balanced with the interests of the ISP.

ISPs have two main interests, although these do overlap considerably. The first is the smooth running of their network. This has obvious economic benefits

48 Article 1(1) Data Protection Directive.

as a functioning network attracts more customers. This is also in the interests of the users as they want and will be paying for access to a working Internet which isn't clogged up with traffic. The second interest of ISPs is to maximise their profits by extracting money from different markets. This would be creating the walled garden Internet described in Section 2. Here they can extract money from content providers and users who want a guaranteed quality of service above and beyond simple Internet access. In this case there is little benefit to the users as they will not be able to access the content that they wish to. It will be even more disadvantageous to users who are not willing, or cannot afford, to pay for a guaranteed service. However in these situations, everyone's personal data will need to be processed even if this is to the users' detriment. In short, the ISPs' interest in extracting more money in this way is directly contradictory to the users' interests in a fully open and accessible Internet.

Therefore, considering the interests of both sides, it is hard to see that the most privacy invasive methods of DPI used to garner an extra income for ISPs will ever outweigh the interests of the data subject. On the other hand, utilising shallow packet inspection techniques, such as using the port number as the basis for discrimination, is not at all privacy invasive as port numbers are not personal data. There can be no argument against this method. The difficulty lies in between these two extremes, within the range of techniques there will become a point where the privacy interests of the user will begin to overtake the interests of the ISP and it is at this point where the processing of personal data is no longer justified. Where this point lies is not clear, and I would suggest that any privacy invasion for the extra profits for ISPs would be hard to justify as there is a clear detriment to a large number of users. This applies to both positive and negative discrimination as defined by Marsden, even where positive discrimination is utilised, all traffic must still be monitored to discover which packets should be put into the fast lane. But, again, in terms of over the top services, there won't be very many situations where such services will be offered without payment and thus the consent of the user. This may not be the case where over the top services are offered free of charge, but this would seem an unusual business model, unless it is a public broadcaster such as NRK or the BBC that are using R2D2 networks to deliver their content. Here consent might not be apparent as any user could access it any point without having entered into a contract with the content provider and thus consented to their ISP prioritising services from that particular content provider.

Therefore, it seems to follow from the DPD that, the only justification for processing personal data for discrimination of Internet traffic (except for reasonable traffic management) is with the users' consent. And this can only be given where there is a suitable choice for the user to make. At its most basic, the choice between having their personal data processed and having no Internet

connection is not a suitable choice, but the choice between accessing or not accessing certain content could be considered as a valid choice, depending on the type of content. This means that any other networks which transit the traffic between sender and recipient will not be able to process personal data for reasons other than reasonable traffic management because it would be impossible for them to have the users unambiguous, or indeed explicit consent, to such processing. There may be an argument that some forms of DPI should be allowed for categorising data without the need for consent, these being the least privacy invasive available. However, as I have mentioned earlier some communications on the Internet will contain sensitive personal data. If some of the data is classed as sensitive then no monitoring can take place without consent as any monitoring will necessarily catch the sensitive data as well.

If the continuous monitoring of communications becomes standard, either through government mandate for security reasons or for the purposes of ever more fine-grained user profile creation for behavioural advertising, the most privacy invasive techniques will likely be used for traffic management and discrimination. If the technology is already installed in the network and being used for one purpose then it will be very tempting for the ISPs to utilise this technology to their own ends as well as others.

4.1.2 Privacy of Electronic Communications

Paul Ohm has written about the potential for DPI to constitute an illegal search under US federal and state wiretap laws,⁴⁹ no such analysis has been done in Europe. I will therefore use the US example as indicative of what could be expected in the EU, the two provisions on either side of the Atlantic are similar in scope.

Ohm notes that, although Network Neutrality and “Network non-Scrutiny”⁵⁰ don’t match up perfectly, there is a significant enough overlap to enable wiretap regulations to restrict ISPs in “total monitoring” which is required for full scale discrimination. The US wiretap laws still allow some scrutiny to take place. They only apply to the actual contents of the packets involved, so shallow packet inspection is still allowed under the wiretap rules. This enables ISPs to monitor data in the packet header such as IP address and port number, but not the actual content of the communication:

49 See e.g. The Federal Wiretap Law 1968 Pub. L. No. 90-350. 82 Stat. 197. as amended by the Electronic Communications Privacy Act 1986 Pub. L. No. 99-508. 100 Stat. 1848; and the Pen Register Act 18 U.S.C. § 3121.

50 Wiretap regulations applied to electronic communications networks.

In a sense, net non-scrutiny gives the ISP one bite of the apple. ISPs may scrutinise (and thus discriminate) between packets so long as the level of scrutiny is low, which may work before the arms race has begun. But once low scrutiny fails to work – because users have started using counter-measures – providers lose the ability to discriminate legally.⁵¹

Similar provisions on the privacy of communications can be found in the Directive on Privacy and Electronic Communications.⁵² Article 5(1) of the Directive states that:

Member states shall ensure the confidentiality of communications and related traffic data by means of a public communications network and publicly available electronic communications services... In particular, they shall prohibit listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data by persons other than users, without the consent of the concerned.” (emphasis added)

A user is defined as “any natural person using a publicly available electronic communications service...”⁵³

There are exceptions to the rule laid out in Article 5(1). These are contained within Article 15(1) of the same directive. They are the usual exemptions to the European privacy regime including those measures which are “necessary, appropriate and proportionate within a democratic society”. This includes national security concerns and the “prevention, investigation, detection, and prosecution of criminal offences or of unauthorised use of the electronic communication system.”

DPI clearly falls under the remit of Article 5(1). It is both intercepting and ‘listening’ to the users’ communication on the Internet. Therefore, for DPI to be allowed it must fall under one of the exceptions in Article 15(1), or be with the consent of the user. There will be times when a network operator becomes aware of certain specific illegal activities going on in their network. In these cases the monitoring, listening, and recording of the content will be legitimate as it will be in the process of investigating and prosecuting a criminal offence. ISPs may also be able to rely on the exceptions for prevention and detection of criminal offences if they wish to maintain constant monitoring of communications, rather than as a response to a confirmed threat. However this would then have to be necessary, appropriate and proportionate in a democratic so-

51 Ohm, 2009 at 1493.

52 Directive 2002/58/EC.

53 Article 2(1).

ciety. It is hard to see that monitoring all communications of all Internet users just in case they are performing some illegal act, such as copyright infringement, being judged to be proportionate. This is following the interest balancing test as describe under Article 7(f) of the Data Protection Directive. It may be reasonable to allow DPI to be utilised if the ISP, the police or a copyright holder have a reason to suspect a certain user is performing illegal acts and gets a warrant from court, but it would not be reasonable to monitor everyone at all times. The threat to users' privacy is too great for mere economic benefits for network access providers. However, again, it could be argued that DPI for reasonable traffic management to combat the threat of congestion on the network could be seen as "necessary, appropriate and proportionate within a democratic society". As mentioned earlier, when considering this test under the Data Protection Directive, the Internet has become a fundamental part of modern life in a democratic society, so keeping it running is in the interests of society as a whole. Discrimination and economic benefit for ISPs is not.⁵⁴ Article 5(1) will still prevent positive discrimination as well as negative discrimination unless consent can be found.

Consent is a justification for monitoring a user's communications as is stated in Article 5(1) above. Article 2(f) of the Directive makes it clear that consent is to be understood in the same way as in the Data Protection Directive, which is discussed above.⁵⁵ It is, however, not clear whether the distinction between personal data and sensitive personal data is recognised under the Directive on Privacy and Electronic Communications. Again, as with the DPD, consent can be given between the user and their ISP as long as there is a real alternative to the data processing carried out by that ISP. This consent can cover both classes of data as long as it is explicit. As stated above, there can be no consent for monitoring by other network providers en route from sender to receiver. This is either due to the lack of choice the user has over the route their data will take or due to the requirement for explicit consent if the distinction between personal data and sensitive personal data is recognised. They cannot choose to have their data sent over networks which do not monitor at all. For monitoring to occur on, for example, tier 1 backbone networks, it will have to be through the exceptions listed in Article 15(1), most notably for national security.

⁵⁴ See section 4.1.1 above.

⁵⁵ See section 4.1.1 above.

4.2 Electronic Communications Law

The provision of Internet access by an ISP falls in the definition of Electronic Communications service as defined by Article 2(c) of the Framework Directive.⁵⁶ Therefore Internet access is covered by the Electronic Communications regime in the EU. The regime includes the Framework Directives and the specific directives;⁵⁷ the most pertinent for this section are the Framework Directive and the Access Directive. The Directive on Privacy and Electronic Communications has been discussed alongside the privacy concerns related to Network Neutrality above. The whole regime has recently gone through a comprehensive review and after much political disagreements over what shape reforms should take⁵⁸ a package was agreed to in December 2009. Two directives⁵⁹ update the old directives in accordance with the review on the performance of the Directives since their inception. These reforms came into force on the 26th May 2011.

To begin with it is important to contrast the position of ISPs and other Internet access providers and content providers. As mentioned above, ISPs fall under electronic communications service providers (Article 2(c) Framework Directive) and, depending on the situation, electronic communications network providers (Article 2(a) Framework Directive). An electronic communications service is a service which “consists wholly or mainly in the conveyance of signals on electronic communications networks... It does not include information society services... which do not consist wholly or mainly in the conveyance of signals on electronic communications networks.” It is clear that ISPs fall under this definition. Their role, at its most basic, is to convey data between content providers and end users. An ISP will also be an electronic communications network provider where it owns the means through which the signals reach the user. So, for example, the old incumbent telecommunications provider (Telenor, BT, etc), Mobile network operators (Telenor, Vodafone, etc), and cable network owners (Canal+, Virgin Media, etc) all fall under this definition. This can be important when it comes to imposing Significant Market Power regulations which I will come back to later.

56 Directive 2002/21/EC on a common regulatory framework for electronic communications networks and services.

57 Directive 2002/19/EC, the Access Directive; Directive 2002/20/EC, the Authorisation Directive; Directive 2002/22/EC, The Universal Service Directive; and Directive 2002/58/EC, the Directive on Privacy and Electronic Communications.

58 See Marsden, 2010, Chapter 5.

59 Directive 2009/136/EC, reforming the Universal Service Directive and the Directive on Privacy and Electronic Communications; and Directive 2009/140/EC, amending the Framework Directive, the Access and Interconnection Directive, and the Authorisation Directive.

Some ISPs also create and host their own content, this, however, along with content providers in general does not fall into this definition. Content providers receive and initiate signals on an electronic communications network, they do not convey them.

Information society services are defined in Article 1(2) of the Information Society Directive⁶⁰ which states:

2). “service”: any Information Society service, that is to say, any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services. For the purposes of this definition:

- “at a distance”: means that the service is provided without the parties being simultaneously present,
- “by electronic means”: means that the service is sent initially and received at its destination by means of electronic equipment for the processing (including digital compression) and storage of data, and entirely transmitted, conveyed and received by wire, by radio, by optical means or by other electromagnetic means,
- “at the individual request of a recipient of services”: means that the service is provided through the transmission of data on individual request.

These definitions covers activities which are carried out over the Internet, for instance access to content on the WWW, VOD services provided over the Internet such as TV2 Sumo or the BBC iPlayer, and P2P file sharing such as that using the BitTorrent system.

So, in short, ISPs are providers of electronic communications service providers and possibly electronic communications network providers. Content providers fall under the category of information society services.

With those definitions in mind I can now look at whether there are any provisions in the regime which attempt to enshrine Network Neutrality as a legal principle, in other words, protect the current neutral Internet. It has been suggested by the European Commission that it is already possible for National Regulatory Authorities (NRAs)⁶¹ to “prevent any blocking of information society services, or degradation in the quality of transmission”.⁶² The commission suggests that Article 5(1) of the Access directive is where such protection

60 Directive 98/34/EC laying down a procedure for the provision of information in the field of technical standards and regulations, as amended by Directive 98/48/EC.

61 The national bodies responsible for regulating the electronic communications regimes.

62 Review of the EU Regulatory Framework for electronic communications networks and services.

can be found. However, it is unclear whether this is actually the case.⁶³ Article 5(1) of the Access Directive states:

“National regulatory authorities shall, acting in pursuit of the objectives set out in Article 8 of [the Framework Directive], encourage and where appropriate ensure, in accordance with the provisions of this directive, adequate access and interconnection, and interoperability of services, exercising their responsibility in a way that promotes efficiency, sustainable competition, efficient investment and innovation], and gives the maximum benefit to end users.” (emphasis added)

So for NRAs to act under Article 5(1) they must be promoting one of the aims set out in Article 8 of the Framework Directive. These are split into three main categories: Article 8(2) concerns promoting competition at the level of electronic communications networks and services; Article 8(3) concerns promoting the development of the internal market; and Article 8(4) deals with promoting the interests of European citizens. Network Neutrality cannot fit into either of the first two categories. As I stated earlier content providers are not classified as electronic service providers so cannot be protected by provisions dealing solely with those services, associated facilities does not include content.⁶⁴ Previous to the review and the subsequent reforms, nothing in Article 8(4) helped with Network Neutrality either. This subcategory deals with things such as data protection and privacy (Article 8(4)(c)) and the provision of clear information (Article 8(4)(d)). However the, following the amendments, a new aim has been added, Article 8(4)(g) states that:

8(4). The national regulatory authorities shall promote the interests of the citizens of the European Union by inter alia:

(...)

(g) promoting the ability of end users to access and distribute information and run applications and services of their choice.

This clearly pertains to Network Neutrality. It indicates that, to an extent, negative network neutrality concerns should be protected by the NRAs.

63 A view shared by the IERG in its Response to Review of Regulatory Framework: “there is some uncertainty about whether existing provisions of the Access Directive are sufficient to deal with the blocking of information society services, especially in cases when these information society services could not be classified as electronic communications services”, Pg 26.

64 Framework Directive, Article 2(e).

However, it would appear to only go so far as promoting simple access to content, so could only covers outright blocking rather than throttling or degrading. It could be argued that degrading access to a type of content below which is necessary to make it function satisfactorily would also constitute denying access to the content. Positive network neutrality concerns are not affected by this aim except possibly where the Internet connection is so poor as to not leave enough bandwidth for access to other services when a prioritised service is used. I will now go on to look at what NRAs can do to promote the aims in Article 8.

Article 5(1) gives the NRAs the responsibility to “encourage and ... ensure access and interconnection, and interoperability”. Access is defined by Article 2(a) of the Access Directive:

2(a) “access” means the making available of facilities and/or services, to another undertaking, under defined conditions, ... for the purpose of providing electronic communications services, including when they are used for the delivery of information society services... (emphasis added).

This is obviously an attempt to give NRAs the power to promote 8(4)(g) above. However, the wording is far from clear in giving them the power to force access to ISPs’ networks by content providers. “[I]ncluding when they are used for the delivery of information society services” defines a subcategory of electronic communications services, and as I have stated above, “electronic communication services” does not include information society services. An electronic communications service which is used for the delivery of information society services is basically an ISP. So, following the wording directly there are no powers attributed to NRAs to force access to an ISP by a content provider.

An alternative potential avenue for Network neutrality regulation can be found in Article 22 of the Universal Service Directive. The third paragraph of the Article states that:

3. In order to prevent the degradation of service and the hindering or slowing down of traffic over networks, Member States shall ensure that national regulatory authorities are able to set minimum quality of service requirements on an undertaking or undertakings providing public communications networks.

Again, this does not create any concrete legal obligations on Member States or NRAs, save that member States must allow NRAs to set minimum quality of

service requirements if they so wish.⁶⁵ It is still unclear as to how NRAs will respond to this provision, whether they will be eager to provide such a minimum requirement; let the market do its job; or feel that it is yet more work an underfunded, understaffed organisation so are unwilling act on it.

If NRAs do act upon this Article then this has the potential to enshrine the entire of Marsden's negative network neutrality concerns into law. Thus making Negative Network Neutrality a legal principle in itself in those jurisdictions where NRAs have acted. Of course, such minimum requirements are likely to be lower than the capacity of an Internet connection will allow, thus permitting throttling a connection to an extent. But if the minimum level is set high enough then the ability to throttle a connection to the extent required to effect user choice, either to be able to extract more money from the consumer or from the content provider, then there will be less or no motivation for ISPs to throttle connections in the search for new revenue streams.

4.2.1 Norway

One NRA which has taken the opportunity to act on Network Neutrality concerns is Norway. The Post- og teletilsynet (NPT), the Norwegian telecommunications regulator, has released a set of guidelines "to ensure that the Internet remains an open and non-discriminatory platform". There are three principles which should be followed, these generally follow the definitions of Network Neutrality given by the Congressional Research Service and by the FCC. They can be summarised as follows:

1. *Internet users are entitled to an Internet connection with a predefined capacity and quality*
2. *Internet users are entitled to an Internet connection that enables them to:*
 - a. *Send and receive content of their choice*
 - b. *Use services and run applications of their choice*
 - c. *Connect hardware and use software of their choice that do not harm the network*
3. *Internet users are entitled to an Internet connection that is free of discrimination with regard to type of application, service or content or based on sender and receiver address.*⁶⁶

⁶⁵ The Article goes on to give the NRAs the responsibility to notify the commission of any requirements that may be put in place and to "take the utmost account" of any feedback from the commission.

⁶⁶ "Network Neutrality: Guidelines for a Neutral Internet", 24th February 2009, NPT, available at <http://www.npt.no/ikbViewer/Content/109604/Guidelines%20for%20network%20neutrality.pdf>. Norsk: http://www.npt.no/ikbViewer/Content/109607/Retningslinjer_for_nettn%C3%B8ytralitet.pdf.

In the guidelines, under principle 3, the non-discrimination principle is qualified by a number of exceptions. These are for, amongst others, normal traffic management and, most importantly for R2D2 networks, for quality of service for certain applications and where the user has consented to the prioritisation of traffic over their connection. Firstly, where a certain application requires quality of service an ISP is not prohibited from doing this under the Guidelines. The Guidelines give two non-exhaustive examples of such applications, namely video and telephony. Secondly, when it comes to the consent of the user, the NPT's definition of consent seems to be in agreement with that of the Data Protection Directive. There must be full notification of the prioritisation services available and that "the users have a real opportunity to choose an Internet connection without prioritisation".⁶⁷ But, again, because of the need for consent there can only be prioritisation over the ISPs network, not other networks, such as tier 1 backbone networks, which happen to transit the data packets on their way from sender to recipient.

4.3 E-Commerce Law

In a number of jurisdictions⁶⁸ ISPs have been granted a certain limit in their liability when it comes to the content which is delivered over their networks. The E-Commerce Directive⁶⁹ sets out 3 areas where an ISPs liability will be limited: "Mere Conduit" (Article 12); "Caching" (Article 13); and "Hosting" (Article 14). It also explicitly states that there shall be no general obligation placed upon ISPs to monitor its users' use of its network (Article 15). This pattern is followed in The US under the Digital Millennium Copyright Act 1998 (DMCA), ISP liability is dealt with in Title II of the Act.

The most relevant of these provisions for Net Neutrality is Article 12 of the Directive; that is treating ISPs as a mere conduit through which data pass to the user.

The whole ISP limited liability regime has been implemented on the presumption that ISP's have no knowledge of what is travelling over their networks and that to impose a duty to monitor all communications is both technically infeasible and would have a major effect on end users privacy and data protection rights. Recital 42 of the E-Commerce Directive states that the

⁶⁷ Principle 3 paragraph B.

⁶⁸ EU, US, and Australia have been looked at.

⁶⁹ Directive 2000/31/EC on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market.

“information society service provider has neither knowledge of nor control over the information which is transmitted or stored.”

The same reasoning is given for providing ISPs with limited liability in Australia. In the case of *Roadshow Films v. iiNet*,⁷⁰ a case dealing with copyright infringement by means of the BitTorrent protocol, the ISP was held to not be liable for the infringement on the grounds of its limited liability as a mere conduit. In his judgement Cowdrey J alluded to the rationale behind the liability rules a number of times, both in respect to the general nature of the workings of the Internet and any reasonable steps that may be taken to prevent copyright infringement by ISPs. “The [ISP] cannot monitor them [infringing copyright] or prevent them from doing so”.⁷¹ “Whether the alleged authoriser has the relevant control or power to prevent the infringements will be determined by the factual matrix present in each case”.⁷² Knowledge and the power to prevent illegal acts are heavily relied on throughout the judgement.⁷³ Finally “due to the transitory nature of the transmission, [an ISP] cannot independently verify the infringing nature of the transmission”.⁷⁴

Even though this area of law isn’t directly applicable to Net Neutrality as such, if ISPs were to begin discriminating against certain types of traffics as described above it could easily be argued that the situation which enables them to enjoy limited liability may be negated. If DPI were to be deployed as standard throughout the network for the purposes of content discrimination then ISPs would have knowledge of the content being transmitted over their networks and with the ability to block, throttle, etc they would have the power to prevent such infringement. By implementing a regime of discrimination ISPs may unwittingly be opening themselves up to increased liability over the content which passes over their network. As Christopher Marsden puts it: “As mere cyphers (sic) for content, [ISPs] are protected; should they engage in any filtering of content they become liable. Thus, masterly inactivity except when prompted by law enforcement is the economically most advantageous policy open to them”.⁷⁵

70 *Roadshow Films Pty Ltd v. iiNet Limited* (No.3) [2010] FCA 24.

71 *Ibid* at 403.

72 *Ibid* at 419.

73 See e.g. *ibid* at 465, 505 & 561.

74 *Ibid* at 594.

75 Marsden, 2010, at 2739.

5 CONCLUSION

Generally Network Neutrality is not protected by any specific regulation in Europe. Norway is the exception here where Network Neutrality is voluntarily protected by the NPT's Guidelines. However, this does leave the door open for discrimination with the consent of the user, thus not prohibiting R2D2 style networks from providing over the top content services on a prioritised basis. This form of regulation, by national NRAs rather than by the EU as a whole, could become more prevalent when the new Electronic Communications reforms are incorporated into national law in 2011.

Network Neutrality is regulated indirectly by a number of different areas of law. Some of these have yet to be rigorously applied to the circumstances, either through court decisions, or further academic research. However, from the plain reading of the various Directives relating to privacy (the Data Protection Directive and the Directive on Privacy of Electronic Communications), it seems clear that Network Neutrality is indirectly regulated to an extent. Only the customer's ISP will probably be allowed to use personal data to prioritise traffic for financial gain, and then only with the consent of the user (which requires there be "open Internet access" available to the customer also). Other ISPs in the chain between sender and recipient will probably not be allowed to use personal data to discriminate for financial gain as there will be no means of garnering consent from the user. Such actions cannot be justified as being more important than the users interests in privacy so will fall foul of the Data Protection rules and constitute an illegal interception under the Directive on Privacy of Electronic Communications.⁷⁶ So, for R2D2 networks, an improved QoE through prioritisation, and thus going against some views of Network Neutrality, will have to pay attention to the privacy related rules. Account will have to be taken of where the prioritisation takes place and exactly what data is required to provide services. Obviously, the less data required for prioritising some data the better and if no personal data is required at all, then the privacy concerns are not at all relevant.

The Electronic Communications regime will regulate against certain forms of negative network neutrality breaches by instigating a minimum quality of service below which ISPs will not be allowed to degrade communications over Internet. This will, to an extent stop ISPs from blocking content and degrading too far, but will still leave considerable scope for degrading below

⁷⁶ The situation regarding illegal interception by DPI technology without consent will be clearer after the Phorm proceedings of the EU Commission are completed.

the quality of other services available over the network. Finally, whilst not affecting Network Neutrality directly, the limited liability provisions under the E-Commerce regime in the EU⁷⁷ may provide some solace for Network Neutrality advocates as ISPs may be reluctant to implement the kind of monitoring for the worst cases of discrimination as such monitoring may lead to them being liable for, amongst other things, breaches of copyright perpetrated by their customers.

⁷⁷ And similar regimes under the DMCA in the US and under Copyright law in Australia.

6 BIBLIOGRAPHY

- Allott Communications, Digging Deeper into Deep Packet Inspection, 2007, available at <https://www.dpacket.org/articles/digging-deeper-deep-packet-inspection-dpi>
- American Civil Liberties Union (ACLU), “Network Neutrality 101: Why the Government Must Act to Preserve the Free and Open Internet”, October 2010
- LA Bygrave, and DW Schartum, “Consent Proportionality and Collective Power” in *S Gutwith et al (eds), Reinventing Data Protection?* (Heidelberg: Springer, 2009) pg 157-175 at 160.
- CRS Report for Congress, Net Neutrality: Background and Issues, 2008, available at: www.fas.org/sgp/crs/misc/RS22444.pdf
- A Cooper, The Singular Challenges of ISP Use of Deep Packet Inspection, 2010, available at <http://www.deeppacketinspection.ca/the-singular-challenges-of-isp-use-of-deep-packet-inspection/#more-68>
- Federal Communications Commission, “Preserving the Open Internet; Report and Order” 76 Federal Register 185 (23rd September 2011) p 59192 – 59235.
- L Lessig, *Code v2* (New York: Basic Books, 2006)
- L Lessig, *Future of Ideas*, (New York: Random House, 2001).
- CT Marsden, *Net Neutrality* (Bloomsbury, 2010). Kindle edition: (A&C Black, 2010)
- NPT, “Network Neutrality: Guidelines for a Neutral Internet”, 24th February 2009, available at <http://www.npt.no/ikbViewer/Content/109604/Guidelines%20for%20network%20neutrality.pdf>. Norsk: http://www.npt.no/ikbViewer/Content/109607/Retningslinjer_for_nettn%C3%B8ytralitet.pdf
- Ofcom, traffic Management and 'Net neutrality', 2010, available at: <http://stakeholders.ofcom.gov.uk/consultations/net-neutrality/>
- P Ohm, “The Rise and Fall of Invasive ISP Surveillance”, *University of Illinois Law Review* 2009, available at <http://ssrn.com/abstract=1261344> at pg 63-65.

JM Peha, The Benefits and Risks of Mandating Network Neutrality, and the Quest for a Balanced Policy, *International Journal of Communication*, Vol. 1, pp. 644-668, 2007.

T Tridimas, *The General Principles of EC Law* (Oxford: OUP, 1999).

J Tollet, Myth 3: Applications Respect Well Known IANA Ports, 2008, available at <https://www.dpacket.org/articles/myth-3-applications-respect-well-known-iana-ports>

T Wu, "Network Neutrality, Broadband Discrimination" *Journal of Communications and High Technology Law*, 2: 141 (2003) available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=388863

Newspaper Articles:

"U.S. Court Curbs F.C.C. Authority on Web Traffic", New York Times, April 6th 2010, available at http://www.nytimes.com/2010/04/07/technology/07net.html?_r=1

"'Transparent' FCC Continues Secret Meetings", *Daily Finance*, June 22nd 2010, available at <http://www.dailyfinance.com/story/company-news/public-interest-groups-appalled-by-closed-door-fcc-web-meeting/19527046/>

"A Face Is Exposed for AOL Searcher No. 4417749", *The New York Times*, August 9th 2006, available at

<http://select.nytimes.com/gst/abstract.html?res=F10612FC345B0C7A8CDDA10894DE404482>

Court Decisions:

Roadshow Films Pty Ltd v. iiNet Limited (No.3) [2010] FCA 24 (Australia)

Legislation:

EU

Directive 2009/140/EC – Better Regulation Directive

Directive 2009/136/EC – Citizens' Rights Directive

Directive 2002/21/EC – Framework Directive

Directive 2002/20/EC – Authorisation Directive

Directive 2002/19/EC – Access Directive

Directive 2002/22/EC – Universal Service Directive

Directive 2002/58/EC – Directive on privacy and electronic communications

Directive 95/46/EC – Data Protection Directive

Directive 2000/31/EC – E Commerce Directive

Directive 98/34/EC – Information Society Directive



RETTSLIGE ASPEKTER VED ANALYSE AV BRUKSMØNSTRE KNYTTET TIL DIGITALE TV-SENDINGER

Dag Wiese Schartum

1 BAKGRUNN

Denne analysen inngår i forskningsprosjektet «Road to media-aware user-Dependent self-aDaptive Networks» (R2D2).¹ Prosjektet har vært finansiert av Verdikt-programmet i Norges forskningsråd, og er et brukerstyrt innovasjonsprosjekt. Hovedmålet for forskningsarbeidet er å utvikle teknikker og verktøy for å modellere, analysere og evaluere brukere og bruksmønstre for bredbåndstjenester, slik at leverandørene kan levere tjenester i henhold til avtalte krav til brukeropplevelse² og teknisk kvalitet³ av disse tjenestene. Følgende delmål for prosjektet er formulert:

1. Videreutvikle metoder og verktøy for modellering av brukere og bruksmønstre av brukertjenester med tilhørende netjtjenester, inkl. metoder og verktøy for datainnsamling og -analyse.
2. Bedre forståelsen av hvordan teknisk kvalitet av netjtjenestene påvirker opplevelsen av brukertjenestene.
3. Utnytte bruker- og brukermønstermodeller for å kunne håndtere, tilpasse og forbedre krav brukeropplevelsen i brukertjenestene og tilhørende teknisk kvalitet i netjtjenester.
4. Utvikle metoder for evaluering av faktisk brukeropplevelse og teknisk kvalitet i bredbåndstjenester, inkludert en forsvarlig håndtering av personvern og andre juridiske forhold mht datainnsamling og bruk.

1 Prosjektet er den norske delen av EUREKA/CELTIC prosjektet R2D2 Networks.

2 Quality of Experience – QoE.

3 Quality of Service – QoS.

Den rettslige analysen i denne rapporten er gjennomført med utgangspunkt i det fjerde delmålet. Analysen er knyttet til digitale, betalte TV-tjenester⁴ med tilhørende netttjenester (heretter, bare «Digital-TV»). I rapporten vil undersøkelse av nettrafikk for å vurdere faktisk brukeropplevelse og teknisk kvalitet av slike tjenester bli omtalt som «trafikkanalyser». Betegnelsen henspeler på analyser av signalstrømmene mellom tjenesteleverandører og brukere.

Av prosjektbeskrivelsen framgår det at den rettslige drøftelsen i stor grad skal gjelde personvern. Det framgår dessuten at også etiske spørsmål skal kunne tas opp i tilknytning til de rettslige drøftelsene. Jeg har valgt å legge avgjørende vekt på å analysere gjeldende rett. I tillegg har jeg gjennomført enkelte rettspolitiske drøftelser, dvs. diskusjoner av om rettsstilstanden er tilfredsstillende, og om det eventuelt er behov for endringer i den rettslige reguleringen.⁵ Etiske problemstillinger er del av slike rettspolitiske overlegninger, og er ikke gjort til separate elementer i analysen.

4 Som for eksempel TV2s Sumo.

5 Se dog kapittel 8 som inneholder noen overordnede rettspolitiske vurderinger.

2 NOEN METODISKE SPØRSMÅL

Størstedelen av dette arbeidet er en undersøkelse og analyse av hvilke rettsregler som er spesielt relevante for gjennomføring av trafikkanalyser med tanke på å evaluere og forbedre brukeropplevelse og teknisk kvalitet ved bruk av bredbånd («trafikkanalyser»). Den hovedsaklige metoden følger således den klassiske rettskildelæren, men jeg kommer ikke her nærmere inn på innholdet av slik rettsdogmatisk metode. Rettskildesituasjonen på området er i utgangspunktet forholdsvis oversiktlig og enkel, idet særlig to lover (ekomloven og personopplysningsloven) spiller en helt sentral rolle. Til lovene er det relativt få rettsavgjørelser⁶ og forarbeidene er relativt viktige. Flere av de konklusjoner jeg trekker er noe usikre. Dette skyldes at trafikkanalyser ikke er en type aktivitet som er direkte regulert i lovene og omtalt i lovforarbeidene, og at de heller ikke ligner på aktiviteter som lovgiver har tatt direkte stilling til. Overføringsverdien av uttalelser i lovforarbeider og uttalelser i dommer mv, er derfor begrenset. Tvil vedrørende rettstilstanden skyldes ikke minst at mange løsninger må finnes ved å kombinere de to nevnte lovene. Lovgiver har ikke vurdert de to lovene i forhold til hverandre, og hva som er korrekte sammenhenger mellom dem er derfor ikke alltid lett å ta stilling til. Det skaper også usikkerhet at forskrifter spiller en forholdsvis stor rolle, og at det til disse verken finnes forarbeider eller rettspraksis. Jeg prøver å angi grad av tvil underveis i drøftelsene.

En metodisk utfordring med et slikt arbeid gjelder utvalg og beskrivelse av de faktiske omstendigheter som skal legges til grunn for drøftelsen. Jeg går ikke inn og vurderer en eksisterende praksis, men har valgt å ta utgangspunkt i en enkel skisse som både er basert på aktuell og mulig praksis. Bak framstillingen ligger det ingen prognose om at tjenestetilbydere vil komme til å forbedre brukeropplevelse og teknisk kvalitet ved å gjennomføre trafikkanalyser knyttet til faktisk bruk av digital-TV. Framstillingen er kun basert på forutsetningen om at dette er én av flere aktuelle strategier. Alternative strategier kommer jeg ikke inn på.

Den følgende framstillingen gjelder mulige trafikkanalyser innenfor rammene av kundeforholdet mellom leverandør er av TV-/nettjenester og brukere/kundene for slike tjenester.⁷ For å unngå at drøftelsen blir spekulativ, har jeg

6 Ingen av disse har blitt ansett å være tilstrekkelig relevante til aktivt å bli trukket inn i drøftelsene.

7 Jeg har for eksempel ikke vurdert trafikkanalyser som er gjennomført i selve forskningsprosjektet.

gjennomført intervjuer hos én nettverksleverandør⁸ og én innholdsleverandør.⁹ Opplysninger fra disse leverandørene inngår i mitt underlagsmateriale, i kombinasjon med opplysninger i prosjektbeskrivelsen for R2D2 og relevant dokumentasjon og litteratur mv. Faktiske forhold jeg legger til grunn er ikke nødvendigvis i samsvar med den informasjonen jeg har mottatt fra de intervjuede tjenesteleverandørene. For det første er det begrenset hvor dypt ned i teknologiske forhold det er nødvendig å trenge. Relevante rettsregler er temmelig generelt formulerte, uten spor av teknologiske spissfindigheter, og er ofte på et helt allment og teknologiuavhengig nivå. Det er derfor ofte begrenset hvor inngående teknologiske beskrivelser kan være for å danne hensiktsmessig grunnlag for rettsdogmatiske drøftelser og finne fram til hvilke rettsregler som gjelder. Informasjon om teknologiske forhold som tjenesteleverandørene har gitt meg har derfor ikke alltid kommet med. Dessuten har jeg i noen tilfelle hatt behov for å tydeliggjøre noen muligheter, og kan derfor ha gjort andre forutsetninger enn det intervjuobjektene har formidlet. Det er derfor grunn til å understreke at framstillingen av forhold vedrørende nettverksleverandører og innholdsleverandører ikke er ment å gi et bilde av de selskapene jeg har innhentet informasjon fra.

8 NTE.

9 TV2 Sumo.

3 NOEN FAKTISKE OG RETTSLIGE UTGANGSPUNKTER FOR DRØFTELSEN

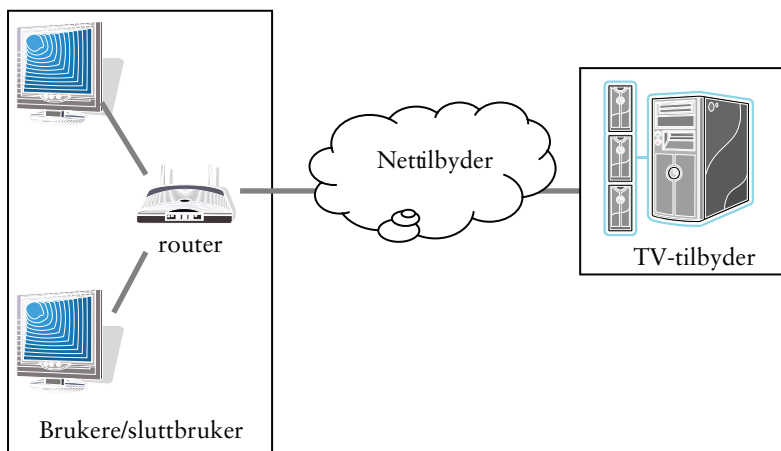
3.1 Overordnet beskrivelse av aktører og tjenester

Den følgende drøftelsen tar utgangspunkt i distribusjon av digital-TV i bredbåndnett. Grovt sett gjelder dette forholdet mellom tre parter: en TV-tilbyder (innholdsleverandør), en nettilbyder og en sluttbruker/abonnent. Hos sluttbruker kan det være flere personer som er brukere av tjenestene og som benytter ulike typer sluttbrukerutstyr (TVer, PCer mv). Tilbyderne kan også tenkes å gjøre bruk av underleverandører, men slike forhold blir bare i begrenset grad tatt hensyn til i det følgende.¹⁰

Jeg legger til grunn at de data som behandles for å levere tjenestene dels kan sies å gjelde trafikkdata, og dels innholdsdata. Innholdsdata er alle data vedrørende lyd og bilde som til sammen utgjør det TV-tilbyder ønsker å levere med best mulig kvalitet og opplevelse, for eksempel en spillefilm. Trafikkdata er data som viser at leveransen skjer/har skjedd, til hvem, til hvilken tid, med hvilken teknisk kvalitet osv. Hvilke trafikkdata som genereres avhenger av hvorledes TV-tilbyder og nettilbyder har satt opp systemene sine, dvs. hvilke hendelser mv systemet er satt opp til å rapportere og loggføre. Jeg forutsetter at trafikkanalyser som denne rapporten omhandler kun gjør bruk av trafikkdata.¹¹

10 For eksempel kan TV-tilbyder gjøre bruk av et «content delivery networks» (CDN), dvs. et nettverk av servere som inneholder etterspurt innhold (f.eks. video og nett-TV), der serverne er plassert på mange punkter i internett. Brukerne aksesserer kopier av ønsket innhold fra en maskin nær dem, i stedet for at alle brukere aksesserer samme sentrale server lenger unna.

11 Jf. omtalen av «deep packet inspection» i Read 2011 (avsnitt 2.2) og mulighetene for å analysere strømmen av datapakker i elektronisk kommunikasjon for ikke bare å identifisere hvilken type kommunikasjon det dreier seg om, men også skaffe seg kunnskap om innholdet av selve kommunikasjonen.



Figur 1

Kvaliteten av tjenesten avhenger av alle de nevnte aktørene. Den tekniske kvaliteten av TV-tilbyderens sending er av grunnleggende betydning for hvilken kvalitet som maksimalt kan mottas hos brukere. Derneft betyr kvaliteten av transportveien, nettet, selvsagt mye. Dårlig kapasitet pga overbelastet nett kan gjøre at den kvaliteten nettilbyder formidler til sluttbruker er utilfredsstillende. Selv om begge leverandører er i stand til å formidle sendinger med ypperlig kvalitet, er også sluttbrukers utstyr avgjørende for om kvaliteten blir god eller ikke. Signalbehandling som skjer på sluttbrukersiden av routeren, ligger i utgangspunktet utenfor tjenestetilbyderens kontroll så lenge avtalen med bruker ikke forplikter bruker til å anvende et bestemt sluttbrukerutstyr. Imidlertid kan det i avtalen med tilbyder være angitt minstekrav til sluttbrukerutstyr som tilbyder anser å være forutsetning for levering i henhold til avtalen.¹² Denne avtalen kan også fastsette noen forutsetninger om den tekniske kvaliteten av nettverksforbindelsen. Også nettverksselskapet kan ha fastsatt tekniske krav til nettverkstjenesten i sine leveringsbetingelser overfor sluttbruker/abonnenten.¹³ Dette er imidlertid to separate avtaleforhold. Manglende kvalitet hos én leverandør kan få konsekvenser for brukerens inntrykk av den andre leverandøren

12 I «Avtale- og brukervilkår for tjenester under TV2.no og andre tjenester levert av eller i samarbeid med TV2 AS hvor TV2 AS er behandlingsansvarlig» gjelder det for eksempel krav til prosessor, operativsystem, minne, skjermkort, nettleter og internettiline. Ved inngåelse av avtalen aksepterer det dessuten at det blir gjort endringer i (bl.a.) tekniske spesifikasjoner og system.

13 I «Alminnelige vilkår for avtale om bredbånd mellom privatkunder og NTE», er det f.eks. i punkt 8.3 avtalt at utstyr sluttbruker kopler til NTEs utstyr mv, skal være anvist/godkjent av NTE.

ytelse, og for bruker vil det være vanskelig å avgjøre om «hakkete» sending skyldes nettselskapet eller TV-selskapet.

Ovenfor nevnte forhold er noe av bakgrunnen for at det kan oppstå behov for å gjøre trafikkanalyser knyttet til leveranse av nett- og TV-tjenester. Helt allment kan opplysninger som sier noe om tjenesten benyttes og hvordan tjenestene framstår/oppleves av brukere, sies å gjelde brukernes privatliv. Enhver indikasjon på private forhold kan neppe sies å være viktig for personvernet. Jo flere, mer detaljerte og sikrere opplysninger nevnte trafikkanalyser kan gi, desto mer problematisk. Derfor er for eksempel analyser som kun kan hente opplysninger fram til sluttbrukers router mindre problematisk enn analyser som også kan hente data fra sluttbrukerutstyret (TV, PC mv). Det følgende er stort sett bygget på forutsetningen om at data knyttet til trafikkanalyser er hentet et sted mellom TV-selskapet og sluttbrukers router. Jeg vil imidlertid ikke utelukke situasjoner der også data knyttet til sluttbrukerutstyr inngår i trafikkanalysen.

Jeg forutsetter at trafikkanalysene skal anvendes for å forbedre brukeropplevelse¹⁴ og teknisk kvalitet¹⁵ av digitale TV-tjenester, men går ikke ut i fra at dette skal skje ved hjelp av bestemte metoder. Prioritering av noe trafikk framfor annen, er én av de foreliggende mulighetene, og kan støte an mot prinsippet om nettverksnøytralitet. Fordi slik prioritering/diskriminering ikke inngår som en forutsetning, blir de heller ikke brakt inn i drøftelsene her.¹⁶

3.2 Overblikk over den rettslige reguleringen

3.2.1 Ekomloven med forskrifter

Distribusjon av digitalt TV over bredbåndsnettet omfattes av lov av 4. juli 2003 nr 83 om elektronisk kommunikasjon («ekomloven», ekoml). Lovens § 1-2 første ledd fastsetter det saklige virkeområdet til bl.a. å gjelde «virksomhet knyttet til overføring av elektronisk kommunikasjon med tilhørende infrastruktur, tjenester, utstyr og installasjoner.» «Elektronisk kommunikasjon» er i loven definert som «overføring av lyd, tekst, bilder eller andre data ved hjelp av elektromagnetiske signaler i fritt rom eller kabel i et system for

14 Quality of Experience – QoE.

15 Quality of Service – QoS.

16 Se Read 2012 om nettverksnøytralitet og personvernmessige vurderinger av å prioritere noe trafikk framfor annen.

signaltransport».¹⁷ I forarbeidene er det fremhevet at loven er teknologinøytral og at den tar hensyn til sammensmelting av teknologier og tjenester («konvergens»). All transmisjonsvirksomhet med tilhørende tjenester er derfor omfattet, uavhengig av om virksomheten kan klassifiseres som telekommunikasjon, informasjonsteknologi eller media.¹⁸ Med kommunikasjon menes i ekomloven enhver informasjon, f.eks. tekst, bilder og lyd, som utveksles eller overføres mellom et begrenset antall personer via en offentlig elektronisk kommunikasjonstjeneste.¹⁹ Fjernsynssendinger som er kringkasting og som går til en ubestemt krets av mottakere, vil med andre ord falle utenfor ekomloven; derimot ikke slike som sendes ut og mottas til bestemte abonnenter (jf «video on demand»).

Loven med forskrifter representerer en omfattende regulering, og i denne rapporten er det bare noen få, utvalgte bestemmelser som vil bli drøftet. Av størst interesse her er at loven fastsetter visse krav om

- Måling og informasjon og kvalitet (§ 2-2)
- Kommunikasjonsvern (§ 2-7) og ekomforskriften kapittel 7
- Taushetsplikt (§ 2-9)

Ekomloven må i utgangspunktet regnes som *lex specialis* i forhold til personopplysningsloven, jf. neste avsnitt. Dersom det oppstår motstrid mellom bestemmelser i de to lovene, vil ekomloven derfor gå foran. Til ekomloven er det gitt forskrifter som bl.a. utdyper bestemmelsene som er nevnt i kulepunktene ovenfor.

3.2.2 Personopplysningsloven med forskrifter

Fordi TV-tjenester som diskuteres i denne rapporten gjelder avtaleforhold mellom tjenestetilbydere og sluttbrukere som går ut på å levere bestemte, utvalgte sendinger, er persontilknytningen ved denne distribusjonsmåten sterkere enn ved kringkastning. Forholdet mellom tjenestetilbydere og sluttbruker kan derfor lettere innebære «behandling av personopplysninger»; dvs. leveransen/bruken av tjenesten genererer opplysninger som kan knyttes til fysiske enkeltpersoner. I så fall kommer også personopplysningsloven med forskrifter til anvendelse. Likevel er det noe uklart når og i hvilket omfang dette er tilfellet. Her vil dette spørsmålet kun bli drøftet i relasjon til trafikkanalyser.

¹⁷ Se ekoml § 1-5 nr. 1.

¹⁸ Se Ot.prp.nr.58 (2002-2003). Om lov om elektronisk kommunikasjon (ekomloven) s 85.

¹⁹ Kringkasting er ikke omfattet, dvs. ekomloven gjelder ikke når signalene sendes til en ubestemt krets av mottakere, jf kringkastingsloven § 1-1 første ledd som bl.a. definerer kringkastning ved at den er «ment eller egnet til å mottas direkte og samtidig av allmennheten».

Personopplysningsloven med forskrifter inneholder en rekke bestemmelser som kommer til anvendelse dersom en kommer til at trafikkanalyser innebærer behandling av personopplysninger. Denne framstillingen er imidlertid begrenset til et mindre utvalg bestemmelser som kan sies å være at spesiell betydning fordi de i) er avgjørende for om loven kommer til anvendelse eller ikke, og ii) fordi trafikkanalyser kan sies å reise spesielle spørsmål. For andre spørsmål knyttet til personopplysningsloven, viser jeg til generelle framstillinger.²⁰

20 Se for eksempel Blixrud og Ottesen 2010 og Schartum og Bygrave 2011.

4 NOEN GRUNNLEGGENDE RETTSSPØRSMÅL

4.1 Oversikt

Som nevnt er det særlig lov om elektronisk kommunikasjon (ekomloven) og lov om behandling av personopplysninger (personopplysningsloven) som er relevante for trafikkanalyser knyttet til digitale TV-tjenester. Langt på vei må disse lovene med tilhørende forskrifter anvendes parallelt. I noen sammenhenger vil regelverkene utfylle hverandre, mens i andre tilfelle vil bestemmelsene i én lov gå foran bestemmelsen i den andre. Begge de norske regelsettene er dessuten basert på EU-direktiver: kommunikasjonsverndirektivet (2002/58/EF) og personverndirektivet (95/46/EF). Disse direktivene vil derfor bli trukket inn i diskusjonene av enkelte spørsmål.

Kapittel 4 i denne rapporten gjelder visse grunnlagsspørsmål som er avgjørende for i hvilken grad de to lovene kommer til anvendelse – hver for seg og i kombinasjon. For lettere å kunne fellesbehandle de to regelsettene, vil jeg først se nærmere på forholdet mellom myndigheter etter de to lovene, og sammenhengen mellom grunnbegreper de to lovene anvender. Derneft går jeg forholdsvis grundig inn i spørsmålet om trafikkanalyser kan anses å være behandling av personopplysninger (avsnitt 4.3). Under forutsetning av bekreftende svar på dette, går jeg nærmere inn på krav til rettslig grunnlag for å bruke personopplysninger i trafikkanalyser, og spesielt spørsmål knyttet til samtykke. Alle disse spørsmålene må uansett være avklart før trafikkanalyser kan starte.

4.2 Hovedaktører og stedlig virkeområde

4.2.1 Oversikt

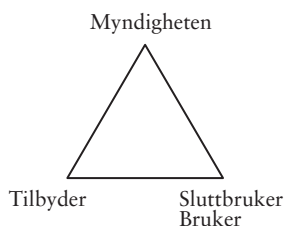
Ekomloven identifiserer og definerer aktører som inngår i elektronisk kommunikasjon. På tilsvarende måte identifiserer og definerer personopplysningsloven aktører som inngår i elektronisk behandling av personopplysninger. Definisjonene av disse aktørene er delvis overlappende, men altså ikke identiske. Når ekomloven definerer aktøren «bruker» gjør den for eksempel det på en måte som åpenbart omfatter aktører som er «registrert». Samtidig er det klart at det er flere «registrerte» som kan knyttes til en digital TV-sending enn de som er «bruker» etter ekomloven. Det oppstår med andre ord behov for å

klargjøre forholdet mellom de ulike aktørene i de to lovene. Klargjøringen er også en forutsetning for korrekt forståelse av samspillet mellom andre bestemmelser i de to lovene.

Ekomloven gjelder generelt for Norge, mens avgjørende for personopplysningslovens stedlige virkeområde er hvor «behandlingsansvarlig» er etablert. Siden stedlig virkeområde for den ene loven er så nært knyttet til aktørene, har jeg valgt også å inkludere denne drøftelsen i gjennomgangen av aktørene.

Hvis vi først ser på ekomloven, inneholder den legaldefinisjoner av aktørene «bruker», «sluttbruker» og «tilbyder».²¹ Myndighet etter loven er i § 1-4 fastsatt til Kongen, departementet og Post- og teletilsynet (PT). Samtidig gis Kongen myndighet til å bestemme at andre offentlige organer eller private skal ha myndighet på begrensede områder. Den myndigheten med størst betydning for gjennomføringen av loven, er åpenbart PT. Post- og teletilsynet har stor grad av selvstendighet, og kan i noen sakstyper ikke instrueres av overordnet myndighet, se § 10-2.²²

Figur 2



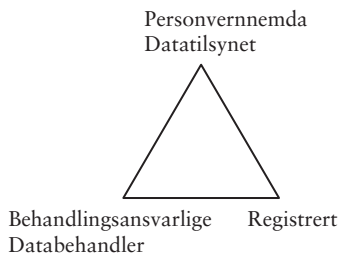
Denne selvstendigheten gjelder imidlertid ikke saksområder som er spesielt relevante for problemstillinger i denne rapporten. Tilbyder etter loven er enhver som tilbyr andre tilgang til elektronisk kommunikasjonsnett eller -tjeneste. Dette omfatter for eksempel nettselskap og innholdsleverandører som for eksempel TV-selskap. Sluttbruker er enhver som har inngått avtale om tilgang til elektronisk kommunikasjonsnett eller -tjeneste. Begrepet omfatter åpenbart enhver privatperson som har inngått avtale om bredbåndstjenester og TV-tjenester. Bruker er i hovedsak definert som enhver som bruker elektronisk kommunikasjonsnett eller -tjeneste. Det kan med andre ord være knyttet mange brukere til en sluttbruker. Til et TV-tilbud kan sluttbruker (abonnenten) for eksempel tenkes å gi tilgang til programmene for en lang rekke mennesker; både medlemmer av husstanden (familie, leieboere) og andre (venner osv).

Etter personopplysningsloven er det Datatilsynet og Personvernemnda som er myndigheter, dvs. som bl.a. kan gjøre vedtak i enkeltsaker. Datatilsynet har det løpende tilsynet med at loven blir etterlevet. Personvernemnda er et kollegialt organ som behandler klager på enkeltvedtak Datatilsynet har truffet. Nemndas praksis har relativt stor vekt ved fortolkningen av loven.

21 Se henholdsvis ekoml. § 1-5 nr 12, 13 og 14. I det følgende vil jeg bruke «tjenestetilbyder» synonymt med «tilbyder».

22 Dette gjelder i visse saker om leveringsvilkår, sterk markedsstilling og tilgang til elektroniske nett og tjenester.

Behandlingsansvarlig etter loven er den som bestemmer formålet med å behandle personopplysninger og hvilke hjelpemidler som skal benyttes for å



Figur 3

gjennomføre behandlingen. Dette kan for eksempel være en tilbyder av TV-tjenester som samler inn og behandler opplysninger om sluttbrukere/abonnenter. Den behandlingsansvarlige kan gjøre bruk av oppdragstaker, dvs. av personer eller virksomheter som behandler personopplysninger på vegne av den behandlingsansvarlige.²³ Slike oppdragstakere kalles databehandlere. Registrert person er en fysisk person som en personopplysning kan knyttes til. For eksempel kan opplysningen om betaling for et bestemt program knyt-

tes til en sluttbruker, og denne sluttbrukeren (abonnenten) blir åpenbart også registrert person.

I det følgende vil jeg gi nærmere analyse av forholdet mellom de aktørene som ovenfor er plassert i de respektive hjørnene av de to trekantene. Oppgaven blir med andre ord å se på forholdet mellom myndighetene etter de to lovene, mellom tilbyder og behandlingsansvarlig mv, og mellom sluttbruker/bruker og registrert person. Alle aspekter ved de nevnte relasjonene vil ikke bli drøftet. Framstillingen er dimensjonert i samsvar med behovene i denne forskningsoppgaven.

4.2.2 Forholdet mellom myndighetene

Det er to tilsynsmyndigheter som er særlig aktuelle i tilknytning til trafikkanalyser av digital-TV mv. Post og teletilsynet har tilsyn med ekomloven med forskrifter, i samsvar med bestemmelsene i lovens kapittel 10. Dette omfatter bl.a. overføring av elektronisk kommunikasjon med tilhørende infrastruktur, tjenester, utstyr og installasjoner (jf ekoml § 1-2). Datatilsynet har tilsyn med etterlevelse av personopplysningsloven med forskrifter. Begge tilsyn kan gi pålegg om at forhold som er i strid med lov eller forskrift helt eller delvis skal opphøre, jf hhv ekoml. § 10-6 og pol § 46 siste ledd.

Innen problemområdet for denne rapporten, er de to organenes tilsynsmyndighet overlappende. Post- og teletilsynet har bl.a. tilsyn med brukere og sluttbrukere knyttet til elektronisk kommunikasjon. Disse vil både være fysiske og juridiske personer. Datatilsynet har tilsyn med behandling av personopplysninger. Opplysninger som gjelder fysiske personer er alltid person-

23 Loven stiller krav til avtaleforholdet, se pol § 15.

opplysninger, noe som innebærer at Datatilsynet har tilsynet med den delen av opplysninger om brukere og sluttbrukere som gjelder fysiske personer. Det faktum at tilsynsområdene overlapper, skaper ingen direkte motstridssituasjon. Situasjonen er snarere slik at tilsynsmyndigheten bør utøves koordinert og i samarbeid mellom de to. Tilsynsmodellen innebærer med andre ord at Datatilsynet fører tilsyn med behandling av personopplysninger som tilbydere av elektroniske nett og tjenester har ansvar for.

4.2.3 Forholdet mellom «tilbyder», «behandlingsansvarlig» og «databehandler»

Behandlingsansvarlig er som nevnt «den som bestemmer formålet med behandlingen av personopplysninger og hvilke hjelpemidler som skal brukes» (pol § 2 nr 4). Det er åpenbart at enhver tjenestetilbyder av elektronisk kommunikasjon kan ha slik bestemmelsesrett og derfor må kunne regnes som behandlingsansvarlig. Samtidig kan slike tjenestetilbydere også opptre som oppdragstaker for en annen, for eksempel behandle personopplysninger på vegne av andre tilbydere. Et nettselskapet kan således tenkes å få oppdrag fra en innholdsleverandør om å gjøre analyser av trafikk i sitt nett. Involverer et slikt oppdrag personopplysninger, vil innholdsleverandøren som gir oppdraget være behandlingsansvarlig, mens nettselskapet som er oppdragstaker blir databehandler. En databehandler er alltid en oppdragsgiver som opptrer på vegne av den behandlingsansvarlige, og er aldri en del av den behandlingsansvarliges organisasjon.²⁴ Interne medarbeidere hos den behandlingsansvarlige, kommer med andre ord ikke inn under bestemmelsene om databehandler.²⁵

De som er tilbydere etter ekomloven kan både opptre som aktørene behandlingsansvarlig og databehandler etter personopplysningsloven. Hva de konkret må regnes som, avhenger av en nærmere analyse av hva behandlingen går ut på og innholdet av avtaleforholdet.

Her kommer jeg ikke inn på spørsmålet om de nærmer detaljerte kriteriene for å bli regnet som tilbyder, behandlingsansvarlig og databehandler.²⁶ Jeg nøyer meg med å presisere på enkelte punkter der det erfaringsmessig ofte oppstår tvil.

Både behandlingsansvarlig og databehandler kan prinsipielt sett tenkes å være en enkeltperson, men i de sammenhengene vi her drøfter, er det i praksis

24 Jf pol § 2 nr 5. Forholdet mellom behandlingsansvarlig og databehandler må derfor reguleres i avtale. Behandlingsansvarlig kan ikke instruere en databehandler med mindre avtalen gir rett til det.

25 For slike medarbeidere gjelder det visse bestemmelser i personopplysningsforskriften vedrørende informasjonssikkerhet, se nærmere om dette i avsnitt 5.2 (nedenfor).

26 Se for eksempel Schartum og Bygrave 2011, s 144- 155 om de to sist nevnte begrepene.

tale om organisasjoner, dvs. kommersielle virksomheter. I så fall kan begge aktører konkretiseres til å være virksomheten ved dets øverste ledelse. Ikke sjelden er virksomheter del av en større selskapsstruktur, noe som kan gjøre det uklart hvor høyt opp i strukturen en må gå for å finne behandlingsansvarlig. Valget vil typisk stå mellom et datterselskap og moderselskapet.

Skillet mellom moder- og datterselskap er primært knyttet til definisjonen av «behandlings-ansvarlig». Definisjonen lyder: «den som bestemmer formålet med behandlingen av personopplysninger og hvilke hjelpemidler som skal brukes» (pol § 2 nr 4). Definisjonen er med andre ord knyttet til *avgjørelser* om hva opplysningene skal brukes til og hvilken programvare mv som skal brukes for å gjennomføre behandlingen. Siden formuleringen «som bestemmer» er brukt, kan det tyde på at en sikter til den som *faktisk bestemmer*, i motsetning til den som formelt har myndighet til å bestemme. Ingen av disse ytterpunktene kan legges til grunn; dvs. en kan ikke bare se på enten formelle eller faktiske forhold. Til tross for ordlyden er det imidlertid grunn til å legge størst vekt på formelle forhold. Spørsmålet blir da hvem som har øverste beslutnings-myndighet i spørsmål som gjelder formål og hjelpemidler for å behandle personopplysningene. Den som ikke kan bli instruert av andre om hvorledes behandling av personopplysninger skal skje, vil således være behandlingsansvarlig. Med dette som utgangspunkt, må en også legge vekt på faktiske forhold. Dersom det for eksempel foreligger en langvarig praksis for at en underordnet organisasjon har behandlingsansvaret, og overordnede instanser i organisasjonen ikke har tilstrekkelig interesser eller forutsetninger for å utøve behandlingsansvaret selv, er det mulig ansvaret må kunne legges til et underordnet nivå, selv om overordnet nivå prinsipielt og formelt sett har anledning til å instruere. Jeg antar imidlertid at dette vil være relativt sjeldne unntakstilfelle, og kommer derfor ikke nærmere inn på spørsmålet.

Plassering av behandlingsansvar i toppen av en organisasjon, innebærer selvsagt ikke noen forutsetning om at det faktiske og praktiske arbeidet skal utføres på dette nivået. Poenget er at den øverste ledelsen har en forpliktelse til å organisere (delegere, kontrollere og instruere) behandlingen av personopplysninger på en slik måte at loven vil bli etterlevet.

Fastsettelse av hvem som er behandlingsansvarlig har avgjørende betydning for om norsk lov gjelder for forholdet eller ikke. Personopplysningslovens stedlige virkeområde er i stor grad begrenset til «behandlingsansvarlige som er etablert i Norge». Spørsmålet om den behandlingsansvarlige er etablert i Norge, avhenger av om vedkommende kan sies å utøve en aktivitet gjennom en fast infrastruktur over et ubestemt tidsrom.²⁷ Dersom behandlingsansvarlige for eksempel har et kontorsted i Norge som ikke er rent midlertidig,

27 Se Schartum og Bygrave 2011 s 158 med videre henvisninger til rettspraksis.

vil vedkommende anses å være etablert i landet. I så fall gjelder den norske personopplysningsloven.

Er den behandlingsansvarlige ikke etablert i Norge, men i et annet EU-land, gjelder lovgivningen i vedkommende EU-land i stedet. Er etableringslandet Danmark, er det med andre ord dansk lov som gjelder for behandling av personopplysninger, selv om behandlingen skjer i Norge og gjelder opplysninger om norske borgere. I slike tilfelle vil de nasjonale lovene være basert på samme EU-direktiv om personvern,²⁸ og således ha mange likhetstrekk. Likevel vil det særlig i detaljspørsmål og spørsmål som krever nærmere skjønn, kunne være klare forskjeller mellom landene.²⁹

Når det gjelder trafikkanalyser av digital-TV, må en for eksempel spørre om den øverste bestemmelsesretten vedrørende formål og hjelpemidler for dette arbeidet ligger i en virksomhet som er etablert i Norge. Er svaret ja, gjelder norsk lov. Er det en virksomhet i et EU-land som har behandlingsansvaret, er det dette landets lov som gjelder.

Dersom den behandlingsansvarlige verken er etablert i Norge eller noe annet land i EØS, gjelder norsk lov for all behandling av personopplysninger som skjer med hjelpemidler som er plassert på norsk territorium.³⁰ Slik vil for eksempel trafikkanalyser knyttet til norske sluttbrukere, stort sett komme inn under norsk lov, selv om analysen faktisk styres fra et tredjeland som for eksempel USA. En konsekvens er at personopplysninger fra en slik behandling ikke kan overføres til et tredjeland uten at vilkårene etter norsk lov er oppfylt.³¹

Hvor databehandlere er etablert, spiller i utgangspunktet ingen rolle for valg av lovgivning. Det er med andre ord bare etableringsstedet for den behandlingsansvarlige som er avgjørende, og databehandlere må følge den lovgivningen behandlingsansvarlige er bundet av. Dersom trafikkanalyser utføres av et amerikansk selskap etter oppdrag fra en behandlingsansvarlig som er etablert i Norge, gjelder med andre ord norsk lov for alt hva det amerikanske selskapet foretar seg vedrørende oppdraget. I slike tilfelle kan overføring av personopplysninger til databehandlers (oppdragstakers) hjemland bare skje når det er tillatt etter norsk lov.³² Hva en eventuell databehandler kan foreta seg med de personopplysningene som blir behandlet på vegne av behandlingsansvarlige, skal uttømmende avtales mellom partene i samsvar med pol § 15.

28 Direktiv 95/46/EF.

29 Dette forholdet er en viktig årsak til at EU-kommisjonen har lagt fram forslag til EU-forordning om personvern som skal avløse personverndirektivet fra 1995. En forordning har direkte virkning i EU-landene, og i Norge i samsvar med EØS-avtalen. I så fall blir lovgivningen helt lik i alle land der forordningen har effekt.

30 Unntatt ren overføring/transport av data, se pol § 4 annet ledd.

31 Se pol §§ 29 og 30 om overføring av personopplysninger til utlandet.

32 Se pol §§ 29 og 30.

4.2.4 Forholdet mellom «sluttbruker», «bruker» og «registrert»

Registrert person er betegnelse på den som personopplysningsloven er satt til å beskytte, og den personopplysninger kan knyttes til. Dette vil alltid gjelde en fysisk person.³³ Betegnelsene «sluttbruker» og «bruker» i ekomloven kan både være fysiske og juridiske personer. Derfor er det kun sluttbrukere og brukere i form av enkeltmennesker som er av interesse ved drøftelse av personopplysningslovens betydning for trafikkanalyser.

Sluttbruker er som tidligere nevnt part i avtale om for eksempel levering av bredbåndstjenester og TV-tjenester, dvs. en myndig person med kompetanse til å inngå avtale. Bruker er i vår sammenheng enhver fysisk person som bruker en digital TV-tjeneste med tilhørende netttjenester, herunder også umyndige personer. Sluttbruker vil ofte også være bruker av tjenesten. Det kan være fra én til mange brukere knyttet til hver sluttbruker. Noen brukere vil kunne gjøre temmelig fast og bruk av tjenestene. Dette vil typisk være andre medlemmer av husstanden. Forholdet mellom sluttbruker (typisk mor eller far) og andre brukere i husholdet, kan tenkes å ha preg av å være et fullmaktsforhold: En person i husholdet inngår avtale om levering av tjenester som får konsekvenser for alle medlemmene i husholdet.

Andre personer enn medlemmer av den aktuelle husstanden, kan også regnes som brukere etter ekomloven, men bruken vil typisk være sporadisk og tilfeldig. Dette gjelder for eksempel besøkende hos sluttbruker. Skillet mellom brukere som er medlemmer av husholdet og andre brukere er viktig for spørsmålet hvem det blir behandlet opplysninger om, som ledd i trafikkanalysen. Etter personopplysningsloven er det avgjørende om det kan etableres en tilknytning mellom en opplysning (f.eks. at et TV-program er kjøpt/vist) og en person (at personen P så programmet). Generelt vil sannsynligheten for at husstandsmedlemmer ser på programmer som kjøpes/vises være langt større enn at tilfeldige brukere gjør det samme. Det må derfor legges til grunn at det primært er de brukere som også er medlemmer av husholdet, som er kandidater for å bli regnes som «registrerte personer» etter personopplysningsloven. Jeg kommer tilbake til spørsmålet i avsnitt 4.3.4 (nedenfor).

33 Dvs. i motsetning til «juridisk person» som ofte brukes som betegnelse på virksomheter mv.

4.3 «Behandling av personopplysninger»

4.3.1 Om sammenhenger mellom begreper i de to lovene

Jeg har til nå forutsatt at trafikkanalyser kan innebære «behandling av personopplysninger». Spørsmålet er avgjørende fordi trafikkanalyser som ikke innebærer behandling av personopplysninger ikke kommer inn under personopplysningsloven. Denne loven inneholder en omfattende rettslig regulering, og dersom loven ikke kommer til anvendelse vil det innebære en vesentlig enklere rettslig situasjon enn med motsatt konklusjon. Spørsmålet i dette avsnittet er de nærmere vilkårene for om personopplysningsloven skal komme til anvendelse. Ekomloven kommer uansett til anvendelse dersom opplysningene gjelder elektronisk kommunikasjon.

Personopplysningsloven gjelder primært for behandling av personopplysninger som skjer ved hjelp av *elektroniske hjelpemidler*, se pol § 3 første ledd, bokstav a. Med behandling sikter en til alt som kan utføres av operasjoner på opplysninger, dvs. innsamling, ulike typer manipulering, videresending, lagring mv. Det er ikke tvil om at trafikkanalyser av signalstrømmene knyttet til distribusjon av TV må kategoriseres som «elektronisk». Derfor er ikke tvil om at trafikkanalyser innebærer elektronisk behandling av opplysninger. Det eneste spørsmålet det her er grunn til å drøfte er om den elektroniske behandlingen gjelder opplysninger som kan knyttes til personer (er «personopplysninger»).

Personopplysningsloven definerer personopplysninger som «opplysninger og vurderinger som kan knyttes til en enkeltperson» (§ 2 nr. 1). I tillegg til de definisjonselementer som framgår av denne ordlyden, inneholder forarbeidene og praksis flere andre elementer som er viktige når en skal ta stilling til begrepet. Her vil jeg bare trekke fram de presiseringer som etter min mening er avgjørende for å ta stilling til spørsmål vedrørende trafikkanalyser.

Hva som utgjør en «personopplysning» kan i hovedsak sies å avhenge av tre vurderingstemaer:

- Hva skal regnes som en «person»?
- Hva skal regnes som en «opplysning»?
- Er tilknytningen mellom personer og opplysninger slik at det oppstår en «personopplysning»?

Før jeg går nærmere inn på personopplysningsbegrepet, minner jeg om at spørsmål om personopplysninger i tilknytning til digitale TV-sendinger kom-

mer inn på minst tre måter. Av disse er det kun én som er av stor interesse ved vurderingen av trafikkanalyser.

For det første vil mange sendinger inneholde personopplysninger, dvs. personer opptrer i programmer med bilde og stemme, det kan gis informasjon i programmer om personers private forhold mv. Personvernet til mennesker som opptrer i sendingene er viktig nok, og dekkes delvis av de samme bestemmelser som for trafikkanalysene. Her kommer jeg imidlertid ikke nærmere inn på slike problemstillinger.³⁴

For det andre vil det være personer som utfører og styrer trafikkanalysene. Opplysninger som viser slike personers aktiviteter, herunder hvilke opplysninger de har aksessert og til hvilken tid mv, er eksempler på personopplysninger som bl.a. kommer inn under personopplysningslovgivningen. Slike opplysninger kan for eksempel være grunnlag for å bedømme om personenes handlinger er lovlige, og kan eventuelt være basis for vedtak fra tilsynsmyndigheter og andre reaksjoner. Her kommer jeg ikke inn på spørsmål som særskilt gjelder denne gruppen. Personer som gjennomfører trafikkanalyser vil imidlertid være representanter for aktørene «behandlingsansvarlig» og «databehandler», se nærmere under avsnitt 4.3. De vil derfor komme med i framstillingen av hvilke plikter disse aktørene har for å sikre at lovgivningen blir fulgt.

For det tredje kan personopplysninger gjelde personer som er brukere av TV-tjenestene, dvs. personer som ser og lytter til programmene og eventuelt deltar i interaktive aktiviteter i tilknytning til programtilbud mv. Det er denne personkretsen den følgende diskusjonen primært gjelder. Gruppen er uensartet. Den gjelder i utgangspunktet alle som ser eller hører på programmene mv (jf. «bruker»). Om noen må unntas fordi deres personvern ikke kan sies å være berørt, er et spørsmål som må avgjøres i lys av den følgende diskusjonen av personopplysnings-begrepet.

4.3.2 Om sammenhenger mellom ulike typer data og person-opplysninger

Det som i personopplysningsloven er betegnet «personopplysning» kan inngå som underkategori av data/opplysninger som fremgår i ekomlovens bestemmelser. Således er det i ekomloven anvendt betegnelser på to typer «data»: trafikldata og lokaliseringsdata. En tredje datakategori, «innholdsdata», brukes i straffeprosessloven § 215a. Kategorien er også relevant for, og kan sies å være implisitt i, ekomloven.

Trafikldata er definert som «data som er nødvendig for å overføre kommunikasjon i et elektronisk kommunikasjonsnett eller for fakturering av slik

34 Slike spørsmål gjelder for en stor grad avveiningen mellom ytringsfrihet og personvern. Se om dette bl.a. i NOU 2011: 12 Ytringsfrihet og ansvar i en ny mediehverdag.

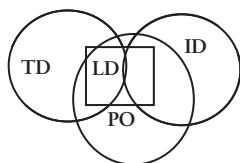
overføring.»³⁵ Begrepet lokaliseringsdata forklares i forarbeidene som «data som behandles i et elektronisk kommunikasjonsnett og som angir den geografiske posisjonen for terminalutstyret til brukeren av en offentlig elektronisk kommunikasjonstjeneste.»³⁶ Dette kan delvis ses som en undergruppe av trafikkdata. Innholdsdata er de dataene (skrift, lyd, bilde mv) som utgjør selve kommunikasjonen; og som uttrykker det meningsinnholdet som en ønsker å formidle.

Vi har dermed tre hovedkategorier data:

- Trafikkdata
- Lokaliseringsdata
- Innholdsdata

Når slike data kan knyttes til en fysisk enkeltperson, vil de inngå i det som ovenfor er forklart som personopplysninger. Etter ekomloven er det ikke noe vilkår at det foreligger personopplysninger. Også data som kun gjelder juridiske personer er omfattet av denne delen av lovgivningen. Personopplysninger vil derfor være en delmengde av slike data som hører inn under de tre datatypene. Ekomloven med forskrifter beskytter altså all elektronisk kommunikasjon uavhengig av om det kan begrunnes ut i fra personvern eller ikke.

Figur 4 illustrerer at trafikkdata (TD) og innholdsdata (ID) i utgangspunktet utgjør to separate områder.³⁷ Lokaliseringsdata (LD) er en delmengde av



Figur 4

trafikkdata (TD), selv om også innholdsdata og personopplysninger ellers kan inneholde opplysninger som gjelder personens oppholdssted. Personopplysninger (PO) kan inngå i alle typer data etter ekomloven, men kan også eksistere separat, uavhengig av den elektroniske kommunikasjonen som trafikkdata, lokaliseringsdata og innholdsdata er knyttet til.

Det er neppe noen helt skarp grense mellom trafikkdata, lokaliseringsdata og innholdsdata. Hvilke opplysninger som er nødvendig for fakturering avhenger for eksempel av hva som i henhold til avtalen med tjenestetilbyder er bestemmende for prising av

35 Se ekomforskriften § 7-1 første ledd.

36 Se ekomforskriften § 7-2, første ledd. Begrepet er også forklart i Ot.prp.nr.58 (2002-2003) Elektronisk kommunikasjon (ekomloven), se merknader til § 2-7. I kommunikasjonsvern-direktivet (2002/58/EF) er «lokaliseringsopplysninger» definert som «alle opplysninger som behandles i et elektronisk kommunikasjonsnett, og som viser den geografiske plasseringen til terminalutstyret til en bruker av en offentlig tilgjengelig elektronisk kommunikasjonstjeneste» (art. 2 (c)).

37 Jf. skillet mellom opplysningene i hodet på en epost og selve meldingsinnholdet i eposten. Skillet er neppe alltid helt klart, men jeg kommer ikke nærmere inn på mulige grensetilfelle her.

tjenesten. Er et priselement knyttet til innholdet, må opplysninger som er nødvendige for faktureringen åpenbart være tilgjengelig for tilbyderer. Betaling kan for eksempel være knyttet til visning av en bestemt film. I så fall må filmen kunne identifiseres og være del av hva tilbyder kan ha lovlig tilgang til for fakturerings-formål. Dermed vil jo også selve innholdet være kjent.

Skillet mellom trafikkdata og innholdsdata får først og fremst betydning og mening når innholdsdata gjelder individuelle og unike ytringer som en abonnent enten sender eller mottar via elektronisk kommunikasjon. Samtidig er det ikke alltid åpenbart at trafikkdata er mindre personverns sensitivt enn innholdsdata: Opplysning om at en abonnent over et lengre tidsrom har bestilt flere fjernsynsprogram med kontroversielt politisk eller religiøst innhold, kan for eksempel ses på som mer sensitivt og beskyttelsesverdig enn opplysninger i en privat, triviell kommunikasjon.

I figuren 4 har jeg forutsatt at lokaliseringsdata delvis er trafikkdata, dvs. nødvendig for at den elektroniske kommunikasjonen kan gjennomføres (et middel). Det kan imidlertid også være et mål i seg selv å generere lokaliseringdata. I så fall kan lokaliseringsdata også ses som innholdsdata. Dersom lokalisering av personer er en separat tjeneste som leveres, kan disse lokaliseringsdataene ses som innholdsdata, dvs. som en del av selve innholdet av telekommunikasjonen (og ikke bare som trafikkdata som må til for sende innholdet til riktig sted).

Diskusjonen ovenfor gir åpenbart problemer i forhold til spørsmål om datalagring slik dette er pålagt i ekoml § 2-7a. Poenget her er nettopp at trafikkdata er noe avgrenset og mindre sensitivt enn andre data. Gjennomføring av datalagringsdirektivet i norsk rett, vil også innebære endring av ekoml. § 2-7 der kategoriene «lokaliseringsdata» og «data nødvendig for å identifisere abonnenten» eksplisitt er innført i tillegg til trafikkdata.³⁸ Den siste kategorien er trolig den samme som ellers i lovproposisjonen er benevnt «abonnementsdata». Når endringene av ekomloven med bakgrunn i datalagringsdirektivet er gjennomført, kan aktuelle data som gjelder elektronisk kommunikasjon deles inn i følgende fire kategorier:

- Abonnementsdata
- Trafikkdata
- Lokaliseringsdata
- Innholdsdata

Problemet med noe flytende overganger mellom kategoriene som nevnt ovenfor, vil imidlertid fortsatt være til stede. Lagringsplikten kan ikke være avhengig av de enkelte abonnentavtalene gjør nødvendig å behandle som trafikkdata,

³⁸ Se ekoml. § 2-7 slik den er vedtatt i lov 15. april 2011 nr. 11 om endringer i ekomloven og straffeprosessloven mv. (gjennomføring av EUs datalagringsdirektiv i norsk rett).

men må eksplisitt angis og begrenses slik at det blir likt for alle tjenestetilbydere. Derfor må forskriften som konkretiserer innholdet av datalagringsplikten direkte angi hvilke data som skal regnes som lagringspliktige trafikkdata. I skrivende stund foreligger ikke slike forskrifter.³⁹

4.3.3 Eksempler på opplysningstyper

I dette avsnittet skal jeg kortfattet gjennomgå opplysningstyper som kan være knyttet til levering av digital-TV til abonnenter. Formålet er å etablere en forholdsvis konkret basis for diskusjon om opplysningene kan være personopplysninger i personopplysningslovens forstand.

Generelle kundeopplysninger er åpenbart personopplysninger, fordi opplysningene gjelder konkrete navngitte personer. Dette kan for eksempel gjelde kontaktopplysninger (navn, postadresse, mobil- og fasttelefonnummer, epostadresse mv), betalingsopplysninger og brukernavn for tjenesten. De fleste kontaktopplysninger samt brukernavn og betalingsopplysninger er obligatoriske fordi de er nødvendige for å inngå og gjennomføre avtalen.

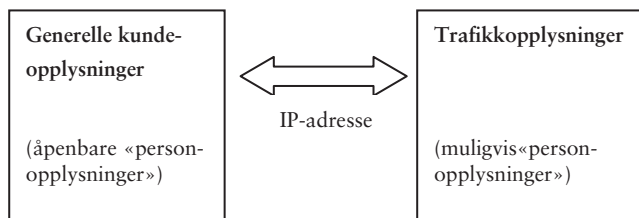
Registrering av opplysninger som ikke er nødvendige for å levere tjenesten, vil stort sett skje på frivillig basis. Dette kan for eksempel gjelde andre personalia enn kontaktopplysninger, samt opplysninger knyttet til markedsundersøkelser, konkurranser og tilleggstenester som krever innlogging. I den grad en velger å utvikle påloggende tjenester, vil det selvsagt være mulig å registrere en lang rekke opplysninger knyttet til hver enkelt brukers identitet, herunder om sammenhengen mellom TV-bruken og andre forbruksvaner og mediebruk. I vår sammenheng er generelle opplysninger om sluttbruker og brukere *i seg selv* relativt lite interessante fordi de åpenbart er personopplysninger. Avgjørende for den personvernmessige vurderingen av trafikkanalyser er trafikkdataene, dvs. opplysninger som beskriver ulike sider ved selve leveransen av innholds- og netjtjenester. I den grad disse opplysningene kan knyttes til opplysninger om sluttbruker og brukere, blir også trafikkopplysningene personopplysninger.

Begrepet trafikkdata er som nevnt definert i ekomforskriften § 7-1 første ledd.⁴⁰ I forarbeidene til ekomloven er trafikkdata videre forklart som «data som angir kommunikasjonens opphavssted, bestemmelsessted, rute, klokke-

39 Se høringsutkast til forskrifter om datalagring, tilgjengelig fra <http://www.npt.no> (publikasjoner/høringer), for eksempel § 2-5 i utkastet som angir lagringsplikt for internettaksess. Plikten omfatter bl.a. «lokaliseringskoden (celleidentiteten) ved kommunikasjonens begynnelse og opplysninger som identifiserer cellens geografiske lokalisering på det tidspunkt dataene blir lagret».

40 Denne første delen av sitatet er tatt inn i ekomforskriften § 7-1 første ledd, annen setning. Siden forskriftsbestemmelsen siterer fra lovforarbeidet, kan definisjonen anses å gjelde felles for både lov og forskrift.

slett, dato, omfang, varighet og underliggende tjeneste.»⁴¹ Ved distribusjon av digital-TV til sluttbrukere, er det for eksempel nødvendig/aktuelt å lagre opplysninger om IP-adresse, kjøpshistorikk (viste programmer, tid, varighet, hvor programmet sees mv), samt en rekke opplysninger av rent teknisk karakter (videoformat, programvare/versjon, direkte sending eller enkeltkjøp av program, hvilke tjenesteleverandører som bidrar, navn på server programmet ses fra mv.). Det er mulig å tenke seg flere opplysningstyper knyttet til abonnement og avspilling av programmer, for eksempel kan en tenke seg innsamling av opplysninger om hvilket avspillingsutstyr og hvilken programvare brukeren benytter.



Figur 5

Poenget i denne sammenheng er at trafikkanalyser kan sies å omfatte én av to sfærer av opplysninger, jf figur 5. I den ene sfæren («Generelle kundeopplysninger») er opplysningene åpenbart personopplysninger, mens spørsmålet er mer tvilsomt for opplysningene i den andre sfæren.

Opplysningene i de to sfærene gjelder delvis samme person(er). Generelle kundeopplysninger er opplysninger om personer som er sluttbrukere/abonnenter og avtalepart med TV-selskap og nettleverandør. Disse opplysningene er direkte navnsatte, og det vil normalt ikke være noen tvil om personenes identitet. Andre opplysninger gjelder datatrafikken i bredbåndsnettet fram til sluttbrukers router, og beskriver hvorledes nett- og TV-tjenester skjer, og om og hvordan tjenestene blir brukt. Jeg forutsetter at disse opplysningene ikke er navnsatte og derfor bare kan knyttes til personer ved hjelp av opplysningen om den IP-adresse de formidlede dataene er knyttet til.⁴² Siden IP-adressen også inngår i de generelle kundeopplysningene, vil det være mulig å finne ut hvilken sluttbruker/abonnent trafikkopplysningene gjelder. Spørsmålet som kan stilles er om den mulighet for identifisering som foreligger via IP-nummeret er nok til at trafikkdataene må regnes som personopplysninger?

For å sette problemstillingen på spissen og maksimalt øke sannsynligheten for at opplysningene *ikke* kan anses å være personopplysninger, vil jeg gjøre

41 Se Ot.prp.nr.58 (2002-2003) s. 92.

42 For eksempel sluttbrukers router.

to forutsetninger. For det første forutsetter jeg at trafikkdataene ligger i et system som er adskilt fra systemet for generelle kundeopplysninger, og at det er strenge rutiner for å sikre trafikkdataenes konfidensialitet. Videre forutsetter jeg at behandling av trafikkdata bare skjer automatisk, og at mennesker bare får tilgang til aggregerte data som er basert på maskinelle analyser av signalstrømmene. Forutsetningen er med andre ord at trafikkanalysen er organisert som en automatisert prosess, adskilt fra andre systemer og prosesser.⁴³

4.3.4 «Personopplysning» og tilknytningskravet

Når behandling av data skjer som ledd i trafikkanalyser, er det primært spørsmålet om tilknytningen mellom personer og opplysninger er slik at det oppstår personopplysninger som byr på tvil (jf. pilen i figur 5). Her vil jeg likevel også kort kommentere de to øvrige hovedvilkårene for at det skal foreligge en personopplysning.

Person. Som nevnt beskytter personopplysningsloven i utgangspunktet bare *levende fysiske personer*. Juridiske personer (virksomheter, organisasjoner) beskyttes ikke som sådanne. Opplysninger som bare sier noe om juridiske personer uten samtidig å si noen om fysiske personer, faller med andre ord utenfor begrepet «personopplysning», og dermed utenfor personopplysningslovens virkeområde. Den nærmere grensegangen mellom fysiske og juridiske personer kommer jeg ikke nærmere inn på. Om det i bestemte situasjoner skjer behandling av opplysninger som kan sies å være i randsonen for hva loven dekker, spiller det neppe noen rolle. Så lenge noen personopplysninger blir behandlet som ledd i trafikkanalyse, kommer hele personopplysningsloven til anvendelse på aktiviteten, uansett om det detaljerte informasjonsinnholdet kan variere.

Opplysning. Alle typer opplysninger er omfattet av begrepet personopplysning; både faktiske forhold (målinger mv) og vurderinger. Opplysningene trenger ikke å være verifiserte eller sanne for å bli regnet som personopplysninger. Det er betydningen av de samlede data som er avgjørende. Hvert sett av data fra trafikkanalyser gir ikke nødvendigvis mening på detaljnivå, men vil kunne gi informasjon når de settes sammen. En forutsetning for at trafikkdata skal kunne regnes som personopplysning er derfor trolig at de kan gis et informasjons-/meningsinnhold (som kan knyttes til en eller flere fysiske personer, jf. nedenfor). Opplysning om visning av et bestemt program gir ikke nødvendigvis personopplysninger av betydning. Den samlede visningen av programmer

43 Det at kundestøtte eller nett- eller TV-selskap undersøker hvorfor en sending for eksempel har dårlig kvalitet, må i så fall gjøre bruk av et annet system enn det som er i bruk for trafikkanalyser.

over tid som viser generelle mønstre for TV-bruken, vil mye klarere være opplysninger av betydning for personvernet.

Det er likegyldig hvorledes personopplysninger kommer til uttrykk. Tekst, tall, grafer, stillbilder, levende bilder, lyd av stemme mv er alt eksempler på aktuelle uttrykksmåter. I tilknytning til trafikkanalyser vil det primært gjøres bruk av tekst, tall og grafer mv, dvs. av uttrykk for personopplysninger som utvilsomt kommer inn under personopplysningsloven.

Tilknytning. For at det skal foreligge personopplysninger, er det nok at opplysninger *kan* knyttes til en fysisk enkeltperson. Det er med andre ord nok at kopling mellom opplysning og person foreligger som en *mulighet*. Likevel gjør ikke enhver teoretisk mulighet for kopling av opplysninger at de regnes som personopplysninger. I fortalen til personverndirektivet heter det således at spørsmålet skal bedømmes ut i fra «alle hjelpemidler [] som det er rimelig å ta i bruk for å identifisere vedkommende, enten av den behandlingsansvarlige eller av en annen person.»⁴⁴ Presiseringen innebærer at opplysninger lettere regnes som personopplysninger dersom den som har tilgang til opplysningene rår over metoder og verktøy for å gjennomføre identifisering. Trafikkdata som befinner seg i teknologiske miljøer der de har kunnskaper, metoder og verktøy mv for å gjennomføre identifisering og knytte dataene opp til enkeltpersoner, vil med andre ord lettere bli vurdert som personopplysninger enn utenfor slike miljøer. Trafikkdata utenfor slike miljøer vil derimot kunne falle utenfor personopplysningsbegrepet dersom sannsynligheten for identifisering er veldig liten fordi de mangler kompetanse, metoder, utstyr mv for å etablere tilknytningen. Miljøer som er aktuelle for trafikkanalyse vil trolig måtte anses å besitte nevnte kompetanse mv, slik at tilknytningskravet lettere vil anses tilfredsstillet enn når andre behandler trafikkdata.

Diskusjonen av hvor vanskelig det skal være å etablere tilknytning mellom en opplysning og en person, kan imidlertid neppe begrenses til spørsmål om kompetanse, metode, tilgang til teknologi og andre teknologisk orienterte elementer. I tillegg er det trolig relevant også å legge vekt på momenter av mer pragmatisk art. Den refererte uttalelsen i direktivets fortale handler om sannsynligheten for at identifisering vil kunne skje. Derfor kan det også hevdes å være relevant å vurdere andre forhold som på forholdsvis sikker måte har betydning for identifisering. Dersom det for eksempel eksisterer et klart forbud mot å gjennomføre identifisering, må dette kunne hevdes å redusere sannsynligheten for at identifisering skjer. På lignende måte kan manglende motivasjon til å identifisere hevdes å redusere sannsynligheten for at det faktisk vil oppstå personopplysninger. Herunder kan utsiktene til straff og erstatning mv være av betydning. Dersom negative konsekvenser av (ulovlig) identifisering er store,

44 Se avsnitt 26 i fortalen til personverndirektivet (95/46/EF).

kan det hevdes å være argument som reduserer sannsynligheten for at identifisering vil skje.⁴⁵ Likevel kan dette neppe være avgjørende momenter, men bare supplere vurderingene knyttet til hovedtemaet om hvilke «hjelpemidler [] [] det er rimelig å ta i bruk for å identifisere», jf nevnte avsnitt i fortalen.

På den annen side må en ta hensyn til skadepotensialet for de personer som det er opplysninger om. I utgangspunktet kan enhver type skade være relevant, men særlig vil skade for personvernet og tilknyttede rettigheter tillegges vekt. Desto mer skadelig det kan hevdes å være dersom det kommer ut opplysning om en person har et bestemt bruksmønster av TV-tjenester e.l., desto sterkere er argumentet for en lite streng forståelse av tilknytningskravet. På lignende måte vil det trolig være relevant å legge vekt på mulig skadelig virkning på informasjonsfriheten. Dersom det er fare for at kunnskap om trafikkanalyser vil gjøre noen mennesker engstelige for at deres TV-bruk skal bli kjent, vil dette kunne være argument for å inkludere opplysninger i gruppen personopplysninger, selv om det er tvilsomt om behandlingsansvarlige rår over nødvendige hjelpemidler, metoder mv. Dette gjelder trolig selv om frykten er irrasjonell; det kan være grunn til å legge vekt på faktiske effekter, uten å forutsette at effektene skal ha rasjonelle årsaker.

Dersom det forligger personopplysninger vil personopplysningsloven ofte komme til anvendelse.⁴⁶ En siste type vurdering gjelder betydningen av at personopplysningsloven eventuelt kommer til anvendelse. Dersom det er annen lovgivning eller rettslig beskyttelse som kan hevdes å være tilstrekkelig, taler dette i mot en streng fortolkning av tilknytningskravet. I vår sammenheng kan en for eksempel spørre om det er behov for den beskyttelsen personopplysningsloven gir i tillegg til den beskyttelsen som følger av ekomloven? Mer konkret kan det være relevant å bedømme om sentrale bestemmelser i personopplysningsloven gir mening å anvende på trafikkanalyser, og om de i så fall innebærer et annet og bedre vern enn etter andre regelsett?

Her trekker jeg foreløpig ingen konklusjon mht. om tilknytningskravet er tilfredsstillt eller ei i tilfelle der det skjer trafikkanalyse av signaler vedrørende digital TV. Først er det behov for å beskrive den persongruppen som kan sies å ha et vernebehov, jf. neste avsnitt. Deretter, i avsnitt 4.3.8 kommer jeg tilbake til spørsmålet om begrepet personopplysning og om personopplysningsloven gjelder for trafikkanalyser.

45 Dette gjelder ikke bare i forhold til straffereaksjoner og krav på erstatning mv, men også faktiske negative konsekvenser i form av dårlig renommé og tap av markedsandeler mv.

46 Det er også enkelte andre krav som må være oppfylt, men i tilknytning til trafikkanalyser kan vi regne med at disse som oftest er tilfredsstillt.

4.3.5 Nærmere om den aktuelle personkretsen som person-opplysningene kan gjelde

Personopplysningsbegrepet forutsetter som nevnt at en kan identifisere fysiske personer, dvs. etablere en viss grad av sikkerhet for hvem personene er. Manglende kunnskap om identiteter og mulighet for å autentisere, kan føre til at opplysningene likevel ikke kan regnes som personopplysninger.

I det følgende går jeg ut i fra at TV-tjenesten ikke er knyttet til personlig visningsutstyr. Hadde tjenesten vært det, vil det ikke være særlig tvil om hvilken person som er knyttet til IP-adressen. I stedet går jeg ut i fra at IP-adressen er knyttet til en router som er felles for en hel husstand. I så fall vil én person i husstanden stå som sluttbruker og avtalepart med innholds- og nettleverandørene, og således ha kjent identitet. Øvrige personer som er brukere av tjenestene er derimot i utgangspunktet ukjente. Riktignok kan en lett få opplyst hvilke personer som er registrert bosatt i husholdet, men hvem som faktisk ser programmer i husholdet er likevel grunnleggende ukjent. I tillegg kan det være besøkende som benytter tjenesten.

Situasjonen er med andre ord at det lar seg gjøre å knytte opplysninger i trafikkanalyser til «noen» hos en sluttbruker, men uten at det på forhånd er klart hvem disse personene er. Er det usikkert om opplysningene er knyttet til personene A eller B, vil opplysningen imidlertid fremdeles regnes som personopplysning. Noe usikkerhet med hensyn til identitet gjør med andre ord ikke at opplysningen ikke er personopplysning. Desto flere mulige personer opplysningene kan knyttes til, desto nærmere kommer vi grensen for hva som kan regnes som personopplysning. Kan opplysningene knyttes til én av ti mulige personer, vil det nesten alltid være for stor usikkerhet til at opplysningen kan sies å være personopplysning. I så fall reguleres ikke behandlingen av opplysningen av personopplysningsloven. Dette vil for eksempel være tilfellet i bedrifter der TV-sendingen blir formidlet i felles oppholdsrom mv der mange personer kan oppholde seg.

Dersom det er tale om usikkerhet mht hvilke personer *innenfor et hushold* som opplysningene kan knyttes til, dvs. innenfor en sosial enhet der privatlivet leves, er toleransen for usikkerhet trolig større enn utenfor slike enheter. Usikkerhet om fjernsynsbruk kan knyttes til mor, far eller noen av barna, er derfor neppe avgjørende for spørsmålet om det foreligger personopplysninger, *selv om* antallet barn skulle være høyt. Ofte vil en privat sosial ramme uansett innebære at mye fjernsynsbruk samtidig vil være knyttet til flere personer fra den begrensede private gruppen (familien ser TV sammen, eventuelt sammen med besøkende). Personopplysningsloven har som ett av formålene sine å beskytte privatlivets fred (se § 1 annet ledd). Dette gjør at opplysninger innenfor

en familiemessig ramme lett vil bli ansett å være personopplysninger selv om usikkerheten er stor mht hvilke spesifikke personer opplysningene gjelder.⁴⁷

Når det gjelder spørsmålet om også andre enn de som tilhører husholdet kan regnes som registrerte personer, viser jeg til drøftelsen under avsnitt 5.3.1.⁴⁸

I forhold til trafikkanalyser i forbindelse med digitale TV-sendinger må forutsetningen være at analysene skjer til ulike tidspunkt og perioder, og uavhengig av kunnskap om hvilke personer som faktisk er i huset og – mer eller mindre – følger sendinger. En rettslig bedømmelse må derfor gå ut i fra at den faktiske situasjonen foran skjermen kan være alt fra at én person «sover foran TVen» til at hele husstanden med mange besøkende følger konsentrert med.

4.3.6 Bred hensiktsmessighetsvurdering

Spørsmålet om trafikkanalyser skal anses som behandling av personopplysninger med den konsekvens at personopplysningsloven kommer til anvendelse på aktiviteten, kan også vurderes i lys av hvor hensiktsmessig det kan sies å være at personopplysningsloven gjelder for trafikkanalyser. Spørsmålet er relevant så lenge vi befinner oss i gråsonen for personopplysningsbegrepet, jf særlig spørsmålet om tilknytningskravet i avsnitt 4.2.3. I det følgende velger jeg å drøfte spørsmålet om hensiktsmessighet ut i fra bestemmelser som forutsetter at identiteten til registrerte personer må være relativt lett å fastslå. Dette gjelder i første rekke bestemmelser som gir registrerte personer rettigheter.

I flere tilfelle er behandling av personopplysninger avhengig av samtykke fra den/de registrerte (se §§ 8, 9 første ledd, bokstav a, 30 første ledd bokstav a). I alle slike tilfelle må den behandlingsansvarlige sikre seg at den personen det bes om samtykke fra, virkelig er den registrerte personen. Lignende situasjon oppstår i tilfelle der registrerte person(er) har krav på innsyn og informasjon i samsvar med §§ 18, 22 og 19–21. En behandlingsansvarlig må på tilsvarende måte sikre seg at den som ber om å få opplysninger rettet, slettet eller lignende i samsvar med §§ 27 og 28, virkelig er rett person. Når innsyn og informasjon skal gis, fremgår det av pol § 24 at den behandlingsansvarlige kan kreve «at den registrerte leverer en skriftlig og undertegnet begjæring». I samsvar med kravene til informasjonssikkerhet i § 13 med forskrifter, må

47 Det eneste som kan anses som sikkert, er at en i slike tilfelle vil kunne akseptere et høyere antall mulige personer, sammenlignet med situasjoner utenfor hushold. Også her vil det imidlertid gjelde en øvre grense for hvor mange mulige personer som kan knyttes til en opplysning, for opplysningen likevel ikke regnes som personopplysning.

48 Konklusjonen der er at tilfeldige brukere/gjester i sluttbrukers hushold *ikke* kan ses som bruker etter ekomloven eller registrert person etter personopplysningsloven.

behandlingsansvarlige i tillegg kreve slik autentisering av personer som henvender seg, at konfidensialiteten blir ivaretatt på tilfredsstillende måte.

Alt i alt forutsetter altså en rekke sentrale bestemmelser i personopplysningsloven at det på tilstrekkelig sikker måte er mulig å fastslå hvem personopplysninger gjelder. Dersom vi godtar at opplysningene i trafikkanalyser som beskrevet i avsnitt 4.3.3, er å regne som personopplysninger innebærer det en forutsetning om at det skal være mulig å fastslå hvem som faktisk har sett på TV i de perioder trafikkanalysen gjelder. Som tidligere forklart, er dette ofte høyst usikkert og derfor meget problematisk å gjennomføre.

Dersom vi for eksempel tenker oss at en person i en husstand krever innsyn i trafikkopplysninger vedrørende abonnementet i huset vedkommende bor, er spørsmålet hva som skal til for at slikt innsyn kan gis?⁴⁹ At personen tilhører husstanden er ikke nok til å vite at trafikkdataene gjelder vedkommendes person. Tvert i mot kan innsyn tenkes å gi kunnskap om TV-bruk knyttet til andre personer i husstanden. Gis det innsyn i en slik situasjon, vil innsynet kunne gjelde andre enn den som spør, noe som vil bryte konfidensialitetsvernet for denne andre personen. Med mindre TV-bruken er knyttet til anvendelse av personlig brukerutstyr som autentiserer personene, kan en med andre ord vanskelig bruke personopplysningslovens bestemmelser om innsyn og informasjon i forhold til opplysninger som inngår i trafikkanalyser knyttet til digital-TV.

Tilsvarende problemer oppstår i forhold til samtykke og retting, sletting mv. At slike sentrale lovbestemmelser er meget vanskelig å anvende på trafikkanalyser, kan sies å tale mot at personopplysningsloven bør komme til anvendelse. Argumentet kan derfor brukes mot at opplysninger fra trafikkanalyser skal ses som personopplysninger.

At enkelte av bestemmelsene i loven ikke passer, kan innebære at registrerte personer ikke alltid får det vern og de rettigheter som loven legger opp til. Dersom dette skal få som konsekvens at loven over hodet ikke gjelder, innebærer det at alt vern og alle rettigheter faller bort. Det er etter min mening neppe et holdbart resonnement at en gruppe registrerte personer skal fratas alt vern etter personopplysningsloven fordi det ikke er praktikabelt å gi dem vern/rettigheter i samsvar med deler av denne loven (vedrørende innsyn, informasjon, samtykke mv). Selv om det er relevant å anføre at noen av personopplysnings-

49 Personopplysningsloven § 23 bokstav e har bestemmelse om unntak fra innsyn når opplysningen «utelukkende finnes i tekst som er utarbeidet for den interne saksforberedelse og som heller ikke er utlevert til andre». Trafikkanalyser kan imidlertid bare under helt spesielle forutsetninger ses som intern saksforberedelse.

lovens bestemmelser ikke/vanskelig lar seg gjennomføre på trafikkanalyser, mener jeg derfor dette er argumenter som vanskelig kan tillegges særlig vekt.⁵⁰

4.3.7 Formåls- og behovsvurdering

En annen overordnet tilnærming til spørsmålet om personopplysningsloven får anvendelse på trafikkanalyse av digitale TV-sendinger, er å spørre om det uansett kan sies å foreligge et slikt vern som denne loven gir? Dersom ekomloven kan sies å ivareta personvernet på tilstrekkelig måte, kan dette tenkes å være argument mot at personopplysningsloven bør gjelde i tillegg. Argumentasjonen forutsetter at en ut i fra andre tolkningselementer er i sterkt tvil om personopplysningsloven gjelder eller ikke, for eksempel fordi en er i tvil om tilknytningskravet er oppfylt (jfr avsnitt 4.3.4). Dersom formålet med personopplysningsloven ikke passer med beskyttelsesbehov knyttet til trafikkanalyser, kan denne argumentasjonsmåten tenkes å få noe vekt.

Formålet med personopplysningsloven er «å beskytte den enkelte mot at personvernet blir krenket gjennom behandling av personopplysninger» (§ 1 første ledd). I annet ledd er personvern konkretisert til bl.a. å gjelde «personlig integritet, privatlivets fred og tilstrekkelig kvalitet på personopplysninger». Her er det «privatlivets fred» som er av spesiell interesse. Formålsbestemmelsen kan forstås slik at loven bl.a. skal beskytte behandling av personopplysninger som kan ha innvirkning på privatlivets fred. Det sentrale blir da skadepotensialet på privatlivet. Hva som er en nøyaktig klassifisering av det som kan forårsake skade, er av mindre interesse. Sagt annerledes, desto større skadepotensial det er for privatliv knyttet til behandling av personopplysninger, desto større romslighet vil det være ved bedømmelsen av om opplysningene det gjelder er personopplysninger eller ikke.

Spørsmålet blir etter dette hvilket skadepotensial trafikkanalyser av TV-signaler til husstander kan ha på privatlivet i disse husstandene? Dersom opplysninger om en families bruk av TV-tilbud, som følge av brudd på konfidensialitetsvernet, er det åpenbart stort skadepotensial for en del personer og hushold. Særlig gjelder dette dersom TV-bruken bryter med hvorledes personene prøver/ønsker å framstå i den offentlige sfæren, eller dersom medlemmer av husholdet blir klar over at andre i husholdet har brutt «interne regler» om TV-bruk.

I det følgende forutsetter jeg at det ikke skjer direkte lovbrudd eller alvorlig sikkerhetssvikt hos de tjenesteleverandører som gjennomfører trafikkanalyser. På dette området er det etter min mening langt på vei realistisk å forut-

50 Nedenfor i avsnitt 5.3 og kapittel 7 kommer jeg nærmere tilbake til spørsmålet om hvorledes slike rettigheter som diskutert i dette avsnittet eventuelt kan håndteres.

sette streng regeletterlevelse.⁵¹ Dessuten gir forutsetningen et bilde av den best tenkelige situasjonen, dvs. minst mulig negativ innvirkning på privatliv. Jeg er ikke kjent med noe erfaringsmateriale som kan vise noe om konfliktmuligheter knyttet til trafikkanalyser som berører privatliv. Spørsmålet vil dessuten til en viss grad avhenge av det konkrete opplegget for analyser og aktørenes opptreden, grad av tillit mv. Her kan det derfor bare bli gitt noen antydninger til svar.

Det er neppe grunn til å forutsette at kun reelle feil og forsømmelser knyttet til behandlingen av trafikldata kan gi negative virkninger på privatliv. Analysene forutsetter at aktiviteten er åpent kjent, og derfor er husstandsmedlemmenes oppfatninger uansett av betydning, enten disse er korrekte eller ikke. Rykter og mistanker om at nett- eller TV-selskapet faktisk kan observere hva som velges og vises av TV-programmer hos hver abonnent, er i denne sammenheng like relevant som den korrekte situasjonsbeskrivelsen. Fordi spørsmålet om hva som faktisk skjer er knyttet til avansert teknologi, «svarte bokser» og ikke observerbare prosesser, kan det også være rasjonelt å være skeptisk til om det er samsvar mellom gjeldende regler og praksis. I forhold til personvernet, kan eventuell usikkerhet og manglende tillit hos noen, kunne virke inn på hva de faktisk velger å se på. Særlig er det grunn til å tro at det vil kunne gjelde programmer med politisk, religiøst eller seksuelt innhold. Slik innhold kan være kontroversielt innenfor familier, hushold og sosial gruppe, og kan derfor føre til at personer ikke ønsker å risikere at det blir kjent at de ser TV-programmer som anses som uakseptable. I første omgang berører imidlertid dette primært personenes informasjonsfrihet.

Det neste forholdet som kan gi risiko for negativ innvirkning på personvernet, gjelder den uklarhet som med nødvendighet oppstår mht hvem som faktisk ser på programmer av ulike typer. Frykt for at det kan bli kjent hvilke kontroversielle programmer som er vist i et hjem, kan gi grunnlag for ønske om å kontrollere tilgangen til programmer for andre medlemmer i familien. Slik kontrollbehov og familieinterne regler, kan gi opphav til konflikter som virker negativt inn på privatlivet. Dette er på den annen side en helt ordinær og vanlig konflikt som mange mennesker uansett mener er nødvendig for å ivareta moral, skjerme barn for skadelige inntrykk mv. Poenget i forhold til trafikkanalyser er imidlertid at det er noen utenfor husholdet som forårsaker at spørsmålet kommer opp.

Til slutt er det grunn til å nevne spørsmål knyttet til hvem som har bestemmelsesrett i et hushold vis-à-vis nettselskap og TV-selskap. Poenget er at trafikkanalyser vil kreve en eller annen form for aksept fra noen i husholdet, dvs. av en representant som har rollen som sluttbruker og abonnent.

51 Bl.a. fordi trafikkanalysene i stor grad vil være automatiserte og således ikke avhenge av enkeltpersoners valg i forhold til individuelle abonnenter.

Tjenestetilbyderne kan ikke sjekke om aksept av en avtale eller samtykke fra en person i husholdet skjer ut i fra en enighet mellom alle i husholdet. Det må derfor kunne forutsettes at det i hushold vil være personer som er uenig i og misliker at trafikkanalyser skjer, til tross for at samtykke er gitt.⁵² Slik intern uenighet kan også sies å virke inn på privatlivet.

Selv med en forutsetning om at regler for konfidensialitetsvern mv blir etterlevet 100 %, synes det samlet sett å være et ikke ubetydelig skadepotensial for privatliv ved trafikkanalyser. Mulig negativ innvirkning på informasjonsfrihet fremstår i denne sammenheng som minst like alvorlig som potensialet for skade for personvern og privatliv.

4.3.8 Konklusjon

Utgangspunktet for denne diskusjonen var at det er en viss tvil om opplysningene i trafikkanalyser vil være å anse som personopplysninger slik personopplysningsloven § 2 nr. 1 definerer dette begrepet. Gjennomgangen i avsnittene 4.3.3 og 4.3.4 illustrerer at det til en viss grad er mulig å argumentere for at trafikkanalyser kan legges slik opp at det kommer i randsonen for de sentrale begreper som avgjør om loven gjelder eller ikke. Opplegget i avsnittene 4.3.5 til 4.3.7 var å undersøke om andre mer generelle hensyn kan tenkes å virke i samme retning og dermed danne grunnlag for en konklusjon om at personopplysningsloven på visse vilkår ikke gjelder trafikkanalyser.

Loven forutsetter at en skal ta stilling til spørsmålet i det enkelte tilfellet, og på konkret grunnlag. Så lenge trafikkanalyser ikke er låst fast til et helt standardisert og fast opplegg, kan det derfor ikke gis generelle svar som er helt sikre. Verdien i denne gjennomgangen er derfor først og fremst at det er demonstrert hvorledes analyser av spørsmålet kan legges opp. I denne sammenheng ønsker jeg også å gi en begrunnet prognose for hvorledes konkrete vurderinger av personopplysningsbegrepet i tilknytning til trafikkanalyser vil falle ut.

Etter min mening har det generelt liten eller ingen vekt at deler av personopplysningsloven er lite hensiktsmessig å anvende på opplysninger som inngår i trafikkanalyser (jf avsnitt 4.3.6). I andre sammenhenger hindrer unntaksbestemmelser at samme deler av loven ikke kommer til anvendelse, uten at unntakene svekker relevansen av eller behovet for de resterende bestemmelsene.

Når det gjelder formåls- og behovsanalysen (avsnitt 4.3.7), mener jeg heller ikke den er argument for at personopplysningsloven ikke skal gjelde. For det første representerer ikke ekomloven med forskrifter en særlig regulering som gjør personopplysningsloven overflødig. Dette er en konklusjon som delvis

52 Dette gjelder primært i forhold til mindreårige og gjester i husholdet, se avsnitt 5.3.1 (nedenfor).

kan trekkes på grunnlag av drøftelsene ovenfor, og som dessuten underbygges av drøftelser av konfidensialitetsvern og innsynsrett i kapitlene 5 og 6 (nedenfor). For det andre er det klart at personvernet blir berørt dersom det skjer lovbrudd og opplysningene blir kjent utenfor de aktuelle husholdene. Vi kan riktignok tro at slike brudd vil være veldig lite sannsynlige. Selv med full regelletterlevelse vil imidlertid privatliv kunne bli berørt fordi manglende tillit og (ikke reell) frykt for at opplysningene kommer ut, kan få begrense det frie husstandsmedlemmenes frie valg av TV-programmer, og dermed virkenegativt inn på deres informasjonsfrihet.

Etter min mening er disse vurderingene egnet til å bevege opplysninger i trafikkanalyser ut av den gråsonen som var utgangspunktet etter den grunnleggende analysen av personopplysnings-begrepet. Min prognose er derfor at analyser av nettrafikk knyttet til digitale TV-sendinger vanligvis vil innebære behandling av personopplysninger som kommer inn under personopplysningsloven.⁵³

I den følgende framstillingen legger jeg konklusjonen i dette avsnittet til grunn, og går ut i fra at trafikkanalyser innebærer behandling av personopplysninger. Kapitlene 5–7 (nedenfor) gjelder de mest sentrale krav som i så fall gjelder etter hhv personopplysningsloven og ekomloven.

53 Etter loven og forskriften er det flere unntak fra loven. Ingen av disse er imidlertid relevante for trafikkanalyser.

5 KRAV TIL RETTSLIG GRUNNLAG OG FORMÅLSANGIVELSE

5.1 Oversikt

Både ekomloven og personopplysningsloven kan sies å ha som ideologisk utgangspunkt at opplysninger/data er beskyttet og kan bare gjøres tilgjengelig dersom det er legitimt. Legitimiteten er både knyttet til hvilke framgangsmåter som er nødvendige for å få tilgang («rettslig grunnlag»), og hvilke formål som kan begrunne tilgangen. Spørsmålet om rettslig grunnlag etter personopplysningsloven gjelder for eksempel om det finnes lovhjemmel for å behandle personopplysninger. I mangel av slik hjemmel må en innhente samtykke fra den registrerte, og dersom samtykke ikke er mulig/hensiktsmessig må en kunne vise til en «nødvendig grunn» som angitt i loven.⁵⁴ Formålet med behandlingen av personopplysninger, dvs. hva opplysningene skal brukes til, er en integrert del av spørsmålet om rettslig grunnlag. For at det skal kunne sies å foreligge lovhjemmel, må for eksempel formålet klart framgå av hjemmelen. Ved innhenting av samtykke må en videre sikre at det framgår tydelig for den som samtykker, hva opplysningene skal brukes til. Personopplysningslovens anvisning av hva som kan godtas som «nødvendig grunn»,⁵⁵ er nettopp formulert ut i fra formål (f.eks.: «for å oppfylle en avtale med den registrerte»). I tillegg til å være bestemmende for hva opplysningene kan brukes til, er formålet bestemmende for hvor lenge opplysningene kan behandles⁵⁶ og for hvilke kvalitetskrav som må stilles til opplysningene/dataene.⁵⁷

5.2 Rettslig grunnlag for å behandle trafikkdata

Utgangspunktet er at trafikkdata delvis består av personopplysninger og delvis er opplysninger som gjelder virksomheter. Ekomloven skiller ikke mellom de to kategoriene, men har felles regler for alle trafikkdata. Ekomloven operer ikke med et eksplisitt krav til rettslig grunnlag for å kunne behandle

⁵⁴ Se om dette i Schartum og Bygrave 2011, s. 160-166.

⁵⁵ Se § 8 bokstavene a – f.

⁵⁶ Se § 28.

⁵⁷ Se § 11 første ledd bokstavene d og e.

trafikdata. I § 2-7 annet ledd gir loven imidlertid noen grunnlag selv,⁵⁸ og henviser for øvrig til samtykke fra bruker. Ekomloven opererer med andre ord kun med lovhjemmel og samtykke som mulig rettslig grunnlag for å behandle trafikdata.

Også personopplysningsloven åpner for behandling av personopplysninger/trafikdata på basis av lovhjemmel og samtykke. I tillegg åpner personopplysningsloven for å behandle personopplysninger ut i fra en *nødvendig grunn* som er angitt i lovens § 8. Spørsmålet er da om nødvendig grunn som angitt i personopplysningsloven⁵⁹ kan være rettslig grunnlag for behandling av trafikdata som er personopplysninger? Her uttrykker trolig de to lovene motstridende rettsregler, noe som gjør at den ene loven får prioritet framfor den andre i samsvar med prinsippet om *lex specialis*.

Ekomloven må anses å være uttømmende, og det er ikke holdepunkter for å hevde at nødvendig grunn som rettslig grunnlag kan innfortolkes i denne loven. Ekomloven og personopplysningsloven er basert på hver sine EU-direktiver der det ene direktivet i stor grad viser til det andre. Således heter det f.eks. i avsnitt 10 i fortalen til kommunikasjonsvernordningen⁶⁰ at «In the electronic communications sector, Directive 95/46/EC [personvernordningen] applies in particular to all matters concerning protection of fundamental rights and freedoms, *which are not specifically covered by the provisions of this Directive, ...*» (min kursiv). Spørsmålet om rettslig grunnlag for å behandle trafikdata er regulert i kommunikasjonsvernordningen art. 5 (2), jf art. 15, dvs. av spesielle bestemmelser i dette direktivet. Direktivbestemmelsene etter dette direktivet går foran bestemmelsene i personvernordningen. Tilsvarende må lovbestemmelser som er basert på først nevnte direktiv i utgangspunktet gå foran lovbestemmelser som er basert på sist nevnte direktiv. Konklusjonen er derfor at det bare er lovhjemmel og samtykke som er mulige rettslige grunnlag for å behandle trafikdata. Dette gjelder også når trafikdataene er personopplysninger. I vår sammenheng er det derfor ingen grunn til å drøfte om trafikkanalyser kan baseres på personopplysningslovens bestemmelse i § 8 om nødvendig grunn som rettslig grunnlag.

En gjennomgang av ekomloven gir følgende liste over bestemmelser som kan sies å hjemle tilgang til og behandling av trafikdata uten samtykke:

- Paragraf 2-2 om måling for å informere sluttbruker om kvalitet på tjenester (jf. forskriften kap. 4)

58 Bestemmelsen uttrykker ikke positivt at trafikdata kan brukes for de formål som bestemmelsen nevner, men sier at dataene skal anonymiseres eller slettes dersom de *ikke* lenger er nødvendige for formålene.

59 Se §§ 8 og 9.

60 Direktiv 2002/58/EF.

- Paragraf 2-7 annet ledd om gjennomføring av elektronisk kommunikasjon og tilhørende fakturering
- Paragraf § 2-7a om lagring av trafikkdata og overføring til politi- og påtalemyndigheter⁶¹
- Paragraf 10-3 om avgivelse av opplysninger til myndigheten

I ekomforskriften kapittel 7 om kommunikasjonsvern mv er det dessuten i § 7-1 annet ledd regnet opp formål som tilbyder kan behandle trafikkdata for: Fakturering, trafikkstyring, kundeforespørsler, markedsføring av elektronisk kommunikasjonstjeneste og avsløring av urettmessig bruk av elektronisk kommunikasjon. I bestemmelses siste ledd, heter det at all annen behandling av trafikkdata krever samtykke fra bruker.⁶²

Kulepunktene ovenfor viser selvstendige lovhjemler til å behandle trafikkdata, mens oppregningen i forskriften delvis er en gjentakelse av dette, og innebærer delvis en selvstendig oppregning av formål som ikke krever samtykke. Spørsmålet her er om noen av formålsangivelsene kan sies å dekke trafikkanalyser for å oppnå god brukeropplevelse?⁶³

Et tilsynelatende alternativ er bestemmelsen i ekomloven § 2-2 som kun kortfattet bestemmer at «Tilbyder av offentlig elektronisk kommunikasjonstjeneste skal måle og informere om kvaliteten på tjeneste som tilbys sluttbruker.» Det framgår imidlertid av forarbeidene til loven at denne bestemmelsen gjelder målinger for å legge til rette for sammenligninger mellom ulike tilbydere. Målinger av blant annet «ventetid for installasjoner, reparasjonstid, fremkommelighet, oppkoplingstid, svartid for manuelle tjenester, svartid på nummeropplysning, minimumsantall samtaleautomater i brukbar stand, korrekte regninger mv» er spesielt nevnt.⁶⁴

Det mest aktuelle alternativet er knyttet til begrepet «trafikkstyring» som er nevnt i § 7-1 annet ledd. Trafikkstyring omfatter merking, veivalg og forsendelse av datapakkene over nettet (jf «trafikkflytstyring») for å sikre tilstrekkelig teknisk kvalitet av nettjenesten fram til sluttbruker. Når det derimot gjelder målinger og analyser av hvorledes sluttbrukers utstyr anvendes og fungerer, er det tvilsomt om dette dekkes av begrepet trafikkstyring. Selv om det neppe er klare skiller, blir det ut i fra hensynet til kommunikasjonsvern og personvern mer problematisk jo mer analysene er rettet inn mot og kan fortelle noe om

61 Nærmere bestemmelser om lagringsplikten vil bli gitt ved forskrift.

62 Forskriftsbestemmelsen gjennomfører kommunikasjonsverndirektivet art. 5 (1) siste setning og art. 6 (3). Se også avsnitt 29 og 30 i fortalen til samme direktiv.

63 jf. Quality of Experience – QoE og teknisk kvalitet (Quality of Service – QoS).

64 Selv om eksemplifiseringen passer best på telefoni, er det klart at bestemmelsen gjelder generelt for alle elektroniske kommunikasjonstjenester.

privat utstyr og forhold i den private sfære. Begrepet trafikkstyring er ikke nærmere definert i ekomloven eller -forskriften. Eksisterende ekomregelverk gir derfor ikke utgangspunkt for å fastsette presise grenser mellom det som kan regnes som trafikkstyring slik ekomforskriften § 7-1 annet ledd tillater, og analyse og styring opp mot sluttbrukers utstyr. I stedet må en vurdere reelle hensyn som kan være argument i den ene eller annen retning.

Argumentet for å se på analyse for å bedre brukeropplevelse som del av trafikkstyringen, er at dette ville innebære en relativt billig og smidig fremgangsmåte av trafikkanalysen. I så fall ville tjenesteleverandørene kunne gjennomføre analyser uten samtykke, og derfor uten at analysene skaper oppmerksomhet. Det kan også hevdes å være uhensiktsmessig og plagsomt for brukere dersom de ofte blir bedt om samtykke til behandling av personopplysninger som av mange anses som triviell og uproblematisk. Man kan således hevde at samtykke bør beholdes situasjoner der det har stor betydning, og at trafikkanalyser som forutsatt her ikke hører til den kategorien.

Kommunikasjonsverndirektivet art. 5 (1) annen og tredje setning gir uttrykk for et relativt strengt konfidensialitetsvern for trafikkdata: «[Member states] shall prohibit listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data [...], without the consent of the users concerned [...]. This paragraph shall not prevent technical storage which is necessary for the conveyance of a communication *without prejudice to the principle of confidentiality*.» (min kursiv). Alt som er nødvendig for å befordre telekommunikasjon kan med andre ord gjøres uten den enkeltes samtykke, men bare dersom dette ikke kan være skadelig for opplysningsenes konfidensialitet. Direktivbestemmelsen kan være argument for å forstå forskriften slik at det må være gjennomført en risikovurdering som viser ingen eller minimal risiko for at trafikkanalyser skal føre til konfidensialitetsbrudd.⁶⁵ Er det nevneverdig risiko, skal behandlingen baseres på samtykke.

Et noe annet aspekt ved spørsmålet om unntak fra hovedregelen om samtykke er utdypet i fortalens avsnitt 20. Her heter det bl.a at samtykkekravet «[...] is not intended to prohibit any automatic, intermediate and transient storage of this information in so far as this takes place *for the sole purpose of carrying out the transmission in the electronic communications network* [...]» (min kursiv). Unntaket fra samtykket ser med andre ord ut til å være avgrenset til situasjoner der midlertidig lagring skjer for å gjennomføre den elektroniske overføringen. Dette peker i retning av helt basal behandling av trafikkdata, og indikerer ikke at behandling av trafikkdata for å forbedre overføringen kan skje uten samtykke.

⁶⁵ For trafikkdata som er personopplysninger, følger det av personopplysningsloven § 13 og personopplysningsloven § 2-4 at det uansett alltid skal skje en risikovurdering.

Måling og analyse av trafikkdata opp i mot sluttbrukerutstyr ligger trolig utenfor det de fleste brukere vil ha forventning om at en tjenestetilbyder skal kunne gjøre. Det er derfor uansett grunn til å sikre åpenhet og kunnskap dersom dette faktisk skjer. Vid fortolkning av «trafikkstyring» i en forskriftsbestemmelse og behandling uten samtykke, skaper åpenbart ikke særlig kjennskap om at analysene skjer og forutberegnelighet for brukerne. Endring av forskriften for å tydeliggjøre at slike analyser er tillatt, er én mulighet. Likevel er det åpenbart ikke slik at forskrifter alene er egnet til å skape god kunnskap om rettstilstanden. Det vil trolig ha bedre effekt dersom den enkelte bruker samtykker til at analysene kan skje. Separat samtykke som kun gjelder tillatelse til å gjennomføre trafikkanalyser, kan hevdes å være lite hensiktsmessig fordi det er relativt tungvint og dyrt. Alternativt kan en tenke seg samtykke innhentet i samband med inngåelse av abonnentavtalen. For å sikre valgfrihet, kan dette tenkes å skje ved at sluttbruker og andre brukere i husstanden aktivt velger og aksepterer trafikkanalyse i samband med avtaleinngåelsen. En slik ordning vil gi valgfrihet og kunnskap blant brukere uten at det blir stort ekstra bryderi for tilbydere. Når dette er gjennomførbart, blir det i seg selv et argument mot å behandle trafikkdata uten samtykke.

Avslutningsvis i denne drøftelsen av hvilket rettslig grunnlag som er aktuelt å basere trafikkanalyser på, kan det være grunn til å minne om at begge de relevante lovene på området er basert på prinsipper om stor grad av autonomi og konfidensialitet for den enkelte.⁶⁶ Valg av rettslig grunnlag som ikke kan sies å støtte opp under disse prinsippene, trenger etter min mening en nærmere og relativt sterk begrunnelse. Slik ekomloven med forskrifter nå er utformet, kan jeg ikke se at det er tilstrekkelig sterke argumenter for å tillate gjennomføring av trafikkanalyse uten samtykke fra den enkelte bruker.

5.3 Nærmere om samtykke

5.3.1 Hvem skal samtykke?

I det følgende legger jeg konklusjonen i avsnitt 5.2 til grunn, idet jeg antar at trafikkanalyse krever samtykke. I følge ekomloven § 2-7 annet ledd er det *bruker* som skal gi samtykke. Alle som bruker elektronisk kommunikasjonsnett eller -tjeneste må med andre ord samtykke, jf § 1-5 nr 12. Denne kompetansen avhenger med andre ord av faktisk bruk, og er uavhengig av om det foreligger

66 Jf prinsippet om medbestemmelse, se Schartum og Bygrave 2011, s 103.

avtaleforhold eller ikke.⁶⁷ Dette blir tilsvarende krav som om det hadde stått «registrert» (jf. pol § 2 nr 6) i stedet for «bruker», og innebærer et utgangspunkt om at alle som er brukere av en TV-tjeneste har samtykkekompetanse. En slik regel er lett praktikabel i situasjoner der det gjøres bruk av personlig sluttbrukerutstyr. Når sluttbrukerutstyret for eksempel er felles for en husstand og det ikke skjer noen form for autentisering av den enkelte bruker, kan dette imidlertid bli meget problematisk. For det første vil det neppe være mulig sikkert å bringe på det rene hvem som for eksempel faktisk ser TV-programmer og således er brukere av tjenesten. Selv om det skulle være mulig, kan forholdet være vanskelig å godtgjøre. Videre vil trafikkdata kunne gjelde opplysninger om tjenestebruken over lengre tid, dvs. med et varierende antall konkrete brukere.

En mulig praktisk løsning på samtykkekravet kunne være å stille vilkår om samtykke fra brukerne i abonnementsavtalen. Det kunne for eksempel bety at alle brukere med fast tilhold i husstanden samtykker. Alternativt kunne sluttbruker (abonnent) samtykke på vegne av andre brukere i husstanden. Verken ekomloven eller personopplysningsloven åpner for «stilltiende» eller «konkludent» samtykke, men krever eksplisitt erklæring fra bruker/registrert overfor tjenestetilbyder/behandlingsansvarlig.⁶⁸ I forarbeidene til ekomloven er det eksplisitt forutsatt at samtykke ikke kan forutsettes i abonnementsavtalen: «Samtykket kan ikke utgjøre en del av tilbyders standardvilkår for levering, slik at det fremstår som en betingelse for levering, med mindre dette er helt nødvendig pga. ytelsens art, f.eks. ved lokaliseringstjenester.»⁶⁹ Siden slike trafikkanalyser knyttet til digitalt fjernsyn ikke er «helt nødvendig», er denne uttalelsen i forarbeidene ikke et aktuelt grunnlag for å forutsette samtykke i abonnentavtalen.

«Sluttbruker» vil som regel også være «bruker», dvs. den som står som abonnent vil også være bruker av TV- og netjtjenestene. Selv om ordlyden klart trekker i retning av at det er den enkelte bruker som alltid skal samtykke, tilsier både praktiske forhold og hensynet til personvern og privatliv at en finner fram til en smidigere forståelse. Ikke minst er det grunn til å unngå at enkeltpersoner må redegjøre for eller godtgjøre sin bruk av TV-tjenester for på den måten avgjøre om han/hun må regnes som bruker med samtykkekompetanse.

67 Se ot.prp. nr 58 (2002–2003) der det i merknadene til definisjonen av «bruker» i ekomloven § 2 nr 12 er understreket at det ikke er noen forutsetning at det foreligger direkte avtale med tilbyder, og at en person som for eksempel ringer nødetatens nødnummer, og hvor det ikke foreligger avtale om bruk, vil være bruker i lovens forstand.

68 Se ekomforskriften § 2-4 første ledd og pol § 2 nr 7.

69 Se ot.prp. nr 58 (2002–2003) s 92. Det foreligger neppe noe særpreg ved levering av tjenester i forbindelse med digitalt TV som gjør det nødvendig å forutsette samtykke i standardvilkårene for levering.

Innen en husstand, vil en neppe komme unna kravet om at hver myndig person som bor på adressen må gi sitt selvstendige samtykke. Når det derimot gjelder mindreårige barn som sluttbruker og andre voksne brukere har foreldreansvaret for, vil hver av foreldrene ofte kunne samtykke på vegne av barna. Barns rett til selv å bestemme over personlige forhold, herunder mediebruk, skal etter barnelova gradvis øke i takt med barnets alder og modenhet. Barn under 15 år vil likevel neppe ha noen autonomi i et omfang som har særlig betydning her. Personene med foreldreansvar kan derfor alltid samtykke på vegne av så unge barn.⁷⁰

Når det gjelder barn som har fylt 15 år, må en anta at de fram mot fylte 18 år skal ha en slik selvbestemmelsesrett at de gradvis skal bli fullt ut autonome brukere når de blir myndige.⁷¹ Disse må derfor i utgangspunktet trolig ses som selvstendige brukere i ekomlovens forstand. De har derfor kompetanse til å gi samtykke etter ekomloven, enten sammen med foreldre eller alene. Det er ikke etablert faste aldersgrenser for når barn kan avgi samtykke med full selvstendighet i forhold til foreldre. Trolig må en forstå rettstilstanden slik at den umyndige selv kan avgi samtykke, mens foreldre kan trekke samtykket tilbake når dette kan begrunnes i foreldreansvaret.⁷² Jo eldre barnet er, desto sterkere grunner må en imidlertid anta at foreldre må ha for å kreve samtykket trukket tilbake.

Barnets selvstendighet er større på noen områder enn andre. På områder der lovgiver har gitt barn bestemmelsesrett fra 15 eller 16 år, kan barnet uansett trolig samtykke på egenhånd, og foreldre har neppe rett til å trekke slike samtykker tilbake. Når det gjelder bruk av TV-tjenester, gjelder ingen slik lovbestemt «framskutt selvbestemmelse».

Når det gjelder andre brukere, dvs «tilfeldige personer» som ikke bor i husholdet til sluttbruker (gjester), må også disse i utgangspunktet trolig regnes som brukere i ekomlovens forstand, og således ha samtykkekompetanse i samsvar med § 2-7. En slik forståelse av begrepet vil imidlertid være særdeles upraktisk, og gjør det meget byrdefullt å innhente samtykke knyttet til bruk av TV-tjenester. Nevnte forståelse innebærer dessuten at personene må redegjøre for konkret TV-bruk og sannsynliggjøre at de faktisk så bestemte programmer hos sluttbruker.

Som nevnt vil sluttbruker og bruker ofte også være «registrert» person i samsvar med personopplysningsloven § 2 nr 6. Den registrerte er enkeltpersoner som personopplysninger kan knyttes til, jf § 2 nr 1. Et vilkår for at det

70 Riktignok har barnet rett til å bli hørt (jf barnelova § 31). Manglende dialog med barnet har imidlertid neppe betydning i for gyldigheten av samtykket.

71 Se barnelova § 31.

72 Se om dette i Schartum og Bygrave 2006, s. 139 flg.

kan sies å foreligge personopplysninger er at det må være tilstrekkelig sikker tilknytning mellom opplysningen og personen (dvs. den registrerte). Er det ikke mulig med slik identifikasjon, vil det heller ikke foreligge «personopplysninger» om vedkommende og han vil ikke være «registrert» person.

Siden både ekomloven og personopplysningsloven kommer til anvendelse på opplysninger vedrørende trafikkanalyse av digitale TV-sendinger, kan en spørre om ikke dette identifikasjonskravet smitter over på forståelsen av «bruker» i ekomloven? En person som ser på TV men som det ikke er mulig eller meget vanskelig å identifisere, kan i så fall ikke regnes som «bruker» og er heller ikke «registrert». I så tilfelle har slike personer verken samtykkekompetanse etter ekomloven eller personopplysningsloven.

Den nedre grensen for identifikasjon er i personverndirektivet er angitt ved hjelp av formuleringen «alle hjelpemidler [] som det er rimelig å ta i bruk for å identifisere vedkommende, enten av den behandlingsansvarlige eller av en annen person».⁷³ Dersom tjenestetilbyder eller andre ikke har tilgang til hjelpemidler som kan identifisere «gjestebrukere» i sluttbrukers hjem, vil disse brukerne i så fall ikke være registrert i personopplysningslovens forstand.

Kommunikasjonsverndirektivets begrep «user» dekker fysiske personer.⁷⁴ Samtidig sies det i samme direktivbestemmelse at definisjonene i (bl.a.) personverndirektivet skal gjelde. Med dette som utgangspunkt er det grunn til å anta at opplysninger om brukere som er fysiske personer, alltid er personopplysninger. Den nedre grensen for identifikasjon av brukere etter ekomloven og registrerte etter personopplysningsloven må derfor anses å være sammenfallende. Dersom tjenestetilbyder eller andre ikke har tilgang til hjelpemidler som kan identifisere gjestebrukere i sluttbrukers hjem, vil de således verken være «registrert» eller «bruker». I så fall kreves det ikke samtykke fra disse personene for å gjennomføre trafikkanalyser.

5.3.2 Krav til samtykkeerklæringen

Ekomforskriften § 7-4 første ledd henviser til personopplysningslovens krav til hva som kan godtas som et gyldig samtykke, se pol § 2 nr 7. Dette innebærer at samtykket må være en frivillig, uttrykkelig og informert erklæring fra bruker/den registrerte. Etter ekomloven vil erklæringen gjelde om brukeren godtar behandling av trafikkopplysninger som er knyttet til ham eller henne og som ekomloven ikke gir hjemmel for å behandle uten samtykke. Her går jeg ikke inn på kravet til frivillighet og uttrykkelighet i detalj, men nøyer meg med enkelte presiseringer.

⁷³ Jf. avsnitt 26 i fortalet til personverndirektivet (95/46/EF).

⁷⁴ Se art. 2 (a).

Kravet til *frivillig* samtykke innebærer at det ikke kan være noen sanksjon knyttet til fravær av samtykke. Dette betyr ikke at det ikke kan være negative følger over hode. Blir negative følger *påført* brukere som følge av at samtykke nektes, slik at det kan ses som en reaksjon på nektelsen, er det åpenbart at samtykket ikke kan regnes som frivillig. Tjenestetilbyder/den behandlingsansvarlige må trolig også gjøre en rimelig innsats for å forhindre at nektelse av samtykke gir negative følger, og kan neppe passivt godta negative følger som kan forhindres.⁷⁵ For eksempel kan neppe tilbydere av TV-tjenester bare akseptere at den tekniske kvaliteten av sendinger blir dårlig for brukere som har nektet samtykke til trafikkanalyse, men må i rimelig grad iverksette tiltak som ikke er basert på slike analyser. Hvor stor innsatsen for å unngå negative følger må være er imidlertid umulig å angi generelt.

At samtykket må være *uttrykkelig* innebærer at samtykkebehandlingen må etterlate seg noen påviselige spor som kan dokumentere at samtykket faktisk er gitt. Det gjelder imidlertid ingen formkrav eller andre bestemte krav til framgangsmåter. Trolig åpner dette for at samtykke kan skje via TV-skjermen, slik at bruker kan avgi samtykke ved hjelp av avkrysningsboks, ikon eller lignende. Dersom samtykket skjer på måter som er synlig for alle som ser på skjermen, kan det muligens være grunnlag for å hevde at det eksisterer et fullmaktsforhold: Ett felles samtykke ved hjelp av «avkrysning» på en skjerm alle ser, kan kanskje hevdes å skje på vegne av *alle* brukere på et hvert tidspunkt. Spørsmålet har sammenheng med måten tilbaketrekking av samtykke kan skje. Jeg kommer kort tilbake til dette spørsmålet i neste avsnitt.

Samtykket skal for det tredje være *informert*. Personopplysningsloven har ikke klare regler om hva det skal informeres om. I § 19 er det imidlertid stilt krav til informasjon ved innsamling av personopplysninger, og det er antatt at denne informasjonen herunder må gis ved innhenting av samtykke. Samtykke vil jo nettopp bli innhentet forut for innsamling av personopplysninger fra personen. I ekomforskriften § 7-4 annet ledd er det i tillegg stilt konkrete krav til den informasjonen som skal gis ved innhenting av samtykke til behandling av trafikldata etter ekomloven. Siden begge lover i utgangspunktet gjelder når trafikldata er personopplysninger, skal begge sett av informasjonskrav oppfylles i slike tilfelle. I tabellen nedenfor har jeg sammenstilt informasjonskravene etter de to regelsettene.

⁷⁵ Se Artikkel 29-gruppens «Opinion 15/2011 on the definition of consent», 13. juli 2011 (01197/11/EN, WP187).

Personopplysningsloven § 19	Ekomforskriften § 2-4 annet ledd
navn og adresse på den behandlingsansvarlige og dennes eventuelle representant (<i>jf bokstav a</i>)	
formålet med behandlingen (<i>jf bokstav b</i>)	om formålet med behandlingen
	om behandlingens varighet
	hvilken type trafikk- eller lokaliseringsdata behandlingen gjelder
opplysningene vil bli utlevert, og eventuelt hvem som er mottaker (<i>jf bokstav c</i>)	om lokaliseringsdata er ment å kunne utleveres til tilbyder av tjeneste etter § 7-2, annet ledd
det er frivillig å gi fra seg opplysningene (<i>jf bokstav d</i>)	
annet som gjør den registrerte i stand til å bruke sine rettigheter etter loven her på best mulig måte, som f.eks. informasjon om retten til å kreve innsyn, jf. § 18, og retten til å kreve retting, jf. § 27 og § 28 (<i>jf bokstav e</i>)	

Som det framgår av sammenstillingen er det noen grad av overlapp mellom de to delene av reguleringen. Således gjelder dette særlig kravet til formålsangivelse. Kravet i ekomforskriften om å informere om utlevering av lokaliseringsdata i henhold til ekomforskriften § 7-2 annet ledd, er kun en presisering av den generelt formulerte bestemmelsen i pol § 19 bokstav c. Mens bestemmelsen i ekomforskriften er mest presis med hensyn til adgangen til å utlevere, er personopplysningsloven mest presis på kravet til angivelse av hvem som er mottaker. Frivillighetskravet i pol § 19 bokstav d er en forutsetning for samtykke, og innebærer derfor intet nytt i forhold til samtykkekravet i pol § 2 nr 7. Pålegget i pol § 19 bokstav e om å vurdere hvilken annen informasjon som skal gis, innebærer bl.a. krav om konkret vurdering ut i fra kjennskap til rettighetene etter personopplysningsloven. Her er det mange mulige informasjonselementer som kan være aktuelle. Det kan for eksempel være knyttet spesielle informasjonsbehov til slike trafikkanalyser som er omtalt i denne rapporten. Selv om informasjonen etter § 19 bokstav e er begrenset til

«rettigheter etter loven her», kan dette neppe skarpt avgrenses mot rettigheter etter ekomloven. Siden personopplysningsloven og ekomloven kommer samtidig til anvendelse på samtykke, må vurderingen etter § 19 bokstav e trolig også delvis innbefatte ekomloven.

Det er neppe noen direkte motstrid mellom regelsettene i de to lovene, og derfor ikke behov for å gi enkeltregler prioritet framfor den andre i kraft av prinsippet om *lex specialis* eller lignende. Alle krav (i begge kolonner, se ovenfor) må derfor etterleves ved innhenting av informert samtykke etter ekomloven § 2-7 annet ledd.

Informasjon må logisk sett gis *før* selve den aktive samtykkehandlingen. Ved utforming av samtykkerutiner med bruk av avkrysningsbokser, ikoner eller lignende, er det derfor et poeng å legge til rette for riktig sekvens. Dersom det er lagt godt og synlig til rette for tilbaketrekking av samtykke (uten negative følger) er denne rekkefølgen imidlertid trolig av mindre betydning.

5.3.3 Tilbaketrekking av samtykke

Både ekomforskriften og personopplysningsloven innebærer krav om at samtykke skal kunne trekkes tilbake. Dette er eksplisitt bestemt i ekomforskriften § 7-4, og framgår av forarbeidene til personopplysningsloven.⁷⁶ Ekomforskriften foreskriver at tilbaketrekking av samtykke også skal kunne skje midlertidig for hver oppkopling til det elektroniske kommunikasjonsnettet eller ved hver enkelt bruk av tjenester i dette nettet. Etter personopplysningsloven er det i og for seg ikke noe i veien for at personer som har trukket sitt samtykke kan gi nytt samtykke etter kort tid, slik at tilbaketrekkingen blir midlertidig. Likevel er det ingen bestemmelser i denne loven som krever den grad av fleksibilitet at samtykke kan gis og trekkes tilbake raskt og eventuelt flere ganger. Reguleringen i ekomforskriften § 7-4 er konkret i kravet til fleksibel avgivelse av samtykke, idet det både kreves at ordningen skal være «enkel og vederlagsfri» og at den skal kunne «trekkes tilbake midlertidig for hver oppkobling og tjeneste».⁷⁷ For at disse kravene skal kunne etterleves i praksis, er det trolig nødvendig med høy grad av automatiserte rutiner for avgivelse og tilbaketrekking av samtykke.

Informasjonen som skal gis ved tilbaketrekking av samtykke må trolig omfatte i) når tilbaketrekkingen får effekt og ii) mulige konsekvenser for den som har vært bruker/registrert. I tilknytning til samtykke til å gjennomføre trafikkanalyser, må det trolig forutsettes at effekten er umiddelbar og at det ikke får noen konsekvenser for brukere. De data som er innsamlet fram til

⁷⁶ Se ot.prp. nr 92 (1998-1999), merknader til § 2 nr. 7 i kapittel 16.

⁷⁷ Også personopplysningsloven følger gratisprinsippet, se pol § 17.

Samtykket er trukket tilbake, må imidlertid kunne brukes til angitte formål. Tilbaketrekking av samtykke vil med andre ord ikke ha tilbakevirkende effekt.

Verken ekomforskriften eller personopplysningsloven stiller krav til framgangsmåter ved tilbaketrekking av samtykke. Reelle hensyn, herunder hensynet til forsvarlig saksbehandling, tilsier imidlertid at en i utgangspunktet må legge til grunn de samme krav som ved innhenting av samtykke, dvs. vedrørende frivillighet, uttrykkelighet og informasjon. Av dette følger bl.a. at det ikke må være fastsatt noen negativ følge av å trekke samtykke tilbake, ut over de virkninger som er uunngåelige. Det må trolig også innfortolkes et krav om at tjenestetilbyder/behandlings-ansvarlige viser rimelig grad av aktivitet for å unngå negative konsekvenser. Når det gjelder uttrykkelighet er kravene trolig de samme som ved avgivelse av samtykke.

Dersom vi forutsetter at samtykke kan gis ved hjelp av avkrysningsboks eller lignende på vegne av alle aktuelle brukere i situasjonen, må kravet være at samtykke kan trekkes tilbake på tilsvarende måte, dvs. slik at én bruker kan trekke samtykke tilbake på vegne av alle. Under forutsetning av at tilbaketrekking av samtykke kan skje like lett som avgivelse av samtykke og at dette tydelig framstår som en mulighet for brukerne, er det mulig en slags kollektiv samtykkerutine kan aksepteres både etter ekomloven og personopplysningsloven. Forutsetningen må være at det framgår på skjermen hvis samtykke er gitt, og at personene som er brukere når som helst kan «slå av» samtykke ved et tastetrykk e.l.

Problemet med en slik løsning er at lovgivningen forutsetter *individuelle* samtykker. Med én bruker, vil dette være i varetatt. Er det to eller flere brukere, vil «samtykkestatus» være avhengig av hva brukerne blir enige om. Det vil kunne føre til at personer går med på å akseptere samtykke fordi andre brukere ønsker det, noe som trolig ikke vil tilfredsstillende kravet om frivillighet. Så lenge det ikke skjer noen premiering av brukere som har gitt samtykke til trafikkanalyser, er det imidlertid mest sannsynlig at samtykke ikke vil bli gitt/vil bli trukket tilbake dersom det er uenighet mellom brukere. Etter min mening er derfor en slik samtykkemekanisme innenfor hva det er mulig å akseptere innenfor dagens rettslige regime. For å være aktuell må spørsmålet imidlertid utredes nærmere i forhold til konkrete løsninger.

5.4 Oppsummering

Kravene til rettslig grunnlag for å behandle trafikkopplysninger som også er personopplysninger, følger av ekomloven med forskrifter sammenholdt med

personopplysningsloven. Det er så vidt jeg kan se ikke motstrid mellom de to regelsettene, som på viktige punkter imidlertid supplerer hverandre.

Det grunnleggende rettslige grunnlaget er naturligvis lov. Ekomloven har flere lovgrunnlag for å behandle trafikkopplysninger uten samtykke fra brukere. Min konklusjon er imidlertid at disse hjemlene ikke dekker slik trafikkanalyse knyttet til digitale TV-tjenester som er aktuelle i R2D2-prosjektet. Trafikkanalyser må derfor være basert på samtykke fra brukere. Jeg har imidlertid pekt på flere problemer med å avgrense brukerbegrepet i forhold til mindreårige i husstanden og gjester mv. Dersom innhenting av samtykke som grunnlag for trafikkanalyser skal gjøres unødvendig, trengs det en endring av ekomloven og ekomforskriften. Eventuelle endringer må imidlertid være innen de rammer kommunikasjonsverndirektivet og personverndirektivet setter.⁷⁸

Både ekomregelverket og personopplysningsloven inneholder bestemmelser om hvorledes samtykke kan innhentes for å være gyldige, og hvorledes samtykker kan trekkes tilbake. Gjennomgangen viste både at de to regelverkene gjensidig supplerer hverandre og derfor må anvendes i sammenheng, og at det er flere rettsspørsmål som ikke har en klar løsning. Også på dette punktet kan det derfor være grunn til å vurdere behovet for regelendring; det vil primært si av ekomregelverket.

Det er mulig at det innenfor dagens lovgivning vil være mulig å utforme rutiner for avgivelse og tilbaketrekking av samtykke via skjermen på en måte som tilfredsstiller lovens krav til samtykke fra hver enkelt bruker. En slik ordning krever i alle fall at det er lett synlig for alle brukere om samtykke er «slått på» eller ikke, slik at enhver bruker kan velge å trekke samtykket tilbake ved å «slå av». Arrangementet er strengt tatt ikke helt i samsvar med lovens krav til samtykke, bl.a. fordi det i realiteten kan innebære «flertallsavgjørelser» og samtykke ved passivitet. På den annen side vil en slik ordning trolig gi en langt mer fleksibel og effektiv ivaretagelse av personvernet, enn en samtykkeordning som er basert på en separat, dokumentbasert rutine som klart forholder seg til person for person og disses konkrete TV-bruk. Den beste løsningen vil imidlertid være å gjøre det tydelig i regelverket at nevnte skjermbaserte løsning er mulig.⁷⁹

78 Jeg har ikke vurdert hvilket rom som foreligger for å gjøre endringer mht samtykkekrav mv, men antar generelt at mulighetene er temmelig begrensede.

79 En slik samtykkevariant som klart støtter opp under formålet med loven for øvrig, kan muligens aksepteres innenfor dagens EU-rettslige regime som er basert på direktiver. Det foreligger imidlertid forslag til ny forordning om personvern i EU som skal avløse personverndirektivet. I stedet for samtykkebestemmelser i direktiv, kan vi altså få samtykkebestemmelser som forordning. Forordninger skal gjennomføres i norsk rett «ord for ord» og vil gi lite eller intet slingsringsmonn for særnorske løsninger.

6 SPESIELT OM IVARETAKELSE AV KONFIDENSIALITET

6.1 Oversikt

Ekomloven § 2-9 fastsetter taushetsplikt om «innholdet av elektronisk kommunikasjon og andres bruk av elektronisk kommunikasjon, herunder opplysninger om tekniske innretninger og fremgangsmåter.» Jeg kommer ikke nærmere inn på hvilke opplysninger som mer konkret omfattes av taushetsplikten, men hovedpoenget er at plikten omfatter klart mer enn trafikkdataene. I tillegg til taushetsplikt gjelder et krav om kommunikasjonsvern etter § 2-7. Vernet gjelder selve kommunikasjonen med tilknyttede trafikkdata.

Paragraf 2-9 fastsetter plikt for tilbyder av kommunikasjonsnett og -tjenester til å gjennomføre tiltak for å hindre at uvedkommende får tilgang til opplysninger som er belagt med taushetsplikt. Også etter § 2-7 skal tilbyder «gjennomføre nødvendige sikkerhetstiltak». Bruk av begrepene «kommunikasjonsvern» og «sikkerhetstiltak» i denne bestemmelsen, kan peke i retning av krav til vern av mer enn konfidensialitet, dvs. slik at også andre klassiske elementer i informasjonssikkerhetstiltak som integritet og tilgjengelighet må innfortolkes. Forarbeidene til loven omtaler bare sikring av konfidensialitet, og bestemmelsen i § 2-7 er basert på kommunikasjonsverndirektivet art. 5 om «Confidentiality of the communications».⁸⁰ Dette gjør at andre informasjonssikkerhetskrav for trafikkdata ikke kan anses dekket av ekomloven § 2-7. Sikkerhetskravene etter ekomloven § 2-7 og 2-9 er således av samme type og delvis overlappende med hverandre. Kravene til sikring etter § 2-7 er imidlertid generelt og mer omfattende enn kravene etter § 2-9 som spesielt er knyttet opp til taushetsplikten. Begge bestemmelser er relevante når en skal ta stilling til krav til sikring av trafikkdata, for eksempel i tilknytning til trafikkanalyser.

Trafikkdata som er personopplysninger skal også sikres i henhold til pol § 13. Denne bestemmelsen omfatter også sikring av opplysningenes konfidensialitet, integritet og tilgjengelighet. Her kommer jeg ikke nærmere inn på kravene etter personopplysningsloven for sikring av integritet og tilgjengelighet. Poenget i vår sammenheng er at det gjelder tredobbel regulering av krav til sikring av konfidensialitet når trafikkdataene er personopplysninger.⁸¹ I praksis er det imidlertid sikringskravene i og i medhold av ekoml § 2-7 og pol § 13 som har klart størst betydning, og som jeg i det følgende vil avgrense meg til.

⁸⁰ Direktiv 2002/58/EF.

⁸¹ Dvs. sikringskrav etter ekomloven § 2-7 og § 2-9, og i tillegg pol § 13 med forskrifter.

Det kan neppe tenkes slik motstrid mellom kravene i de to lovene at en må velge det ene regelsettet framfor det andre ut i fra *lex specialis* prinsippet eller lignende. Således legger jeg til grunn at det er *summen* av krav til vern av konfidensialitet etter de to lovene (med forskrifter) som må følges når trafikkdataene er personopplysninger.

Ekomloven § 2-7 annet ledd gjelder spørsmål om anonymisering og sletting av trafikkdata, dvs. tiltak av en annen karakter enn det som er regulert i pol § 13. Anonymisering må trolig forstås i streng mening som et krav om at det ikke lenger skal være mulig å knytte noen enkeltperson til trafikkdataene. Identiteter skal for eksempel ikke kunne tilbakeføres. I så fall vil det ikke lenger foreligge personopplysninger, personopplysningsloven vil ikke gjelde, og pol § 13 om informasjonssikkerhet kommer ikke til anvendelse. Etter anonymiseringen må man trolig forutsette at det heller ikke foreligger trafikkdata, fordi de neppe kan være «nødvendig for overføring av kommunikasjon i et elektronisk kommunikasjonsnett eller for fakturering av slik overføring».⁸² Anonymiserte trafikkdata vil med andre ord falle utenfor det verne-/informasjonssikkerhetsregimet etter ekoml § 2-7 og pol § 13. Opplysningene kan i sjeldne tilfelle trolig likevel være underlagt taushetsplikt og krav til vern etter ekomloven § 2-9. Dette kan tenkes i tilfelle der sammenstilling av anonyme data røper taushetspliktige opplysninger.⁸³

6.2 Grunnleggende plikt til kommunikasjonsvern

Konfidensialitetskravene for trafikkdata følger i stor grad av reglene om taushetsplikt i ekomloven § 2-9. Supplerende konfidensialitetskrav kan imidlertid følge av personopplysningsloven. Således kan ikke trafikkdata som er personopplysninger gis videre dersom ikke formålet med behandlingen begrunner dette, jf avsnitt 4.3.7 (ovenfor). Blir trafikkdata behandlet på grunnlag av samtykke fra bruker, kan spredningen heller ikke være videre enn det samtykket forutsetter (og som det er informert om, jf avsnitt 5.3.2 ovenfor).

Reglene om sikring er gitt for at konfidensialitetskravene skal bli overholdt. Det grunnleggende kravet i ekomloven § 2-7 første ledd innebærer at tjenestetilbyder skal gjennomføre nødvendige tiltak for å sikre konfidensialiteten av kommunikasjon i egne elektroniske kommunikasjonsnett og -tjenester. Kravet

⁸² Jf. definisjonen av trafikkdata i ekomforskriften § 7-1 første ledd.

⁸³ Antagelsen bygger på tilsvarende situasjoner som forutsatt i forvaltningsloven § 13 annet ledd, første setning (jf. «med mindre slike opplysninger røper et klientforhold eller andre forhold som må anses som personlige»).

gjelder i både positiv og negativ forstand, og dekker både tiltak til hva tjenestetilbyder *skal* gjøre for å sikre konfidensialitet og hva han *ikke* skal gjøre. Fordi dette kravet i § 2-7 ikke er nærmere detaljert i ekomforskriften, er det kravene i personopplysningsforskriftens (pof) kapittel om informasjonssikkerhet som får størst betydning.

Ekomloven § 2-7 sammenholdt med pof § 2-4 innebærer at det skal skje en risikovurdering av muligheten for svikt i konfidensialitetsvernet for trafikkdata. Vurderingen skal skje ut i fra en oversikt over alle typer trafikkdata som er personopplysninger. Deretter skal det vurderes sannsynligheten for og konsekvenser av eventuelle brudd på konfidensialitetsvernet av disse opplysningene (antatt risiko). Som grunnlag for risikovurderingen må tjenestetilbyder fastlegge kriterier for *akseptabel* risiko forbundet med behandlingen av trafikkdata som er personopplysninger. Sikringstiltakene skal sørge for at antatt risiko ikke overstiger akseptabel risiko.

Før en kan gjennomføre trafikkanalyser⁸⁴ må det altså ha skjedd en risikovurdering etter § 2-4 i personopplysningsforskriften. Analysen skal dekke mulig svikt når det gjelder krav til konfidensialitet, integritet og tilgjengelighet, men kravene til konfidensialitet har særlig betydning (jf. ekomloven §§ 2-7 og 2-9).

Kravene til sikring av trafikkdata i forbindelse med trafikkanalyser vil trolig være temmelig strenge, dvs. det er ytterst lite risiko som kan aksepteres. Fordi trafikkdata blir underlagt lagringsplikt i samsvar med ekomloven § 2-7a,⁸⁵ og fordi det trolig vil komme til å gjelde forholdsvis detaljerte og strenge sikkerhetskrav i henhold til dette,⁸⁶ vil tjenestetilbyders skjønnsmargin trolig bli vesentlig redusert. Vanligvis er det i stor grad opp til den behandlingsansvarlige å gjøre en risikovurdering ut i fra et forholdsvis vidt skjønn, og fastsette sikkerhetstiltak på grunnlag av dette. Med detaljert angivelse av sikkerhetstiltak i forskrift og konsesjonsvilkår, vil det være forskrifts- og konsesjonsmyndigheten⁸⁷ som utøver mye av skjønn, og valgfriheten for den enkelte tjenestetilbyder blir tilsvarende redusert. Indirekte kan slike myndigheter i så fall sies å angi hva som er akseptabel risiko. Oppdager tjenestetilbyder en risiko som det ikke er tatt høyde for i reguleringen av sikkerhetstiltak, har han imidlertid en selvstendig plikt til å treffe supplerende tiltak ut over det som konkret pålegges i lov, forskrift og konsesjon, jf de generelle kravene i pol § 13.

Tjenestetilbyder skal sikre opplysningene mot innsyn fra uvedkommende. Ekomforskriften § 7-1 annet ledd angir hvilke grupper av personer som kan be-

84 Med samtykke som rettslig grunnlag, jf. avsnitt 5.2 (ovenfor).

85 I forbindelse med gjennomføringen av datalagringsdirektivet.

86 I forskrift til ekomloven og i konsesjoner fra Datatilsynet.

87 Konsesjoner gis av Datatilsynet.

handle trafikkdata uten samtykke fra bruker(e). Personopplysningsforskriften innebærer at det skal fastsettes på personnivå hvem som kan gis tilgang. Således er det bare personer som er autorisert for tilgang og som har fått nødvendig opplæring som kan gis tilgang til trafikkdata som er personopplysninger, se pof § 2-8. Autorisasjonen skal gjelde konkrete, pålagte oppgaver. En person som er autorisert til å behandle trafikkdata for faktureringsformål, kan derfor ikke settes til å behandle dataene for å gjennomføre trafikkanalyser uten utvidet og eksplisitt autorisasjon.

6.3 Sletting

Ekomloven § 2-7 annet ledd, første setning innebærer at trafikkdata som ikke er anonymiserte skal slettes så snart de ikke lenger er nødvendige for kommunikasjons- eller faktureringsformål. Samtykke fra bruker kan likevel gi grunnlag for lengre lagring. Bestemmelsen må uansett forstås slik at det er formålet med behandlingen som bestemmer hvor lenge opplysninger kan lagres.⁸⁸ I den grad trafikkdata skal brukes til trafikkanalyser i henhold til samtykke fra brukere, er det derfor viktig at informasjonen som samtykket bygger på tydelig angir hvor lenge tjenestetilbyder har rett til å bruke opplysningene før de skal slettes.

Også personopplysningsloven inneholder krav om sletting i § 28. I denne bestemmelsen er det vid mulighet for å gjøre unntak fra sletteplikten, og det oppstår derfor motstrid mellom denne bestemmelsen og nevnte bestemmelse i ekomloven. Jeg antar som et utgangspunkt at bestemmelsen i ekomloven § 2-7 annet ledd går foran den lignende bestemmelsen i personopplysningsloven, fordi sist nevnte bestemmelse både er nyest og må anses å være mest spesialisert.

Når § 2-7a om lagringsplikt (jf datalagringsdirektivet) trer i kraft, vil en rekke trafikkdata være lagringspliktige i 6 måneder. Det er viktig å forstå sammenhengen mellom sletteplikten etter § 2-7 og lagringsplikten etter § 2-7a. Både slette- og lagringsplikt må vurderes ut i fra *formål med behandlingen*. Plikt til å slette opplysninger som inngår i trafikkanalyser gjelder analyseformålet, og forhindrer ikke at vedkommende opplysning kan lagres videre for *andre* formål. Det som vil bli lagret etter § 2-7a skjer ut i fra formålet kriminalitetsbekjempelse, og disse opplysningene skal lagres adskilt fra opplysninger som eventuelt behandles for formålet trafikkanalyse.⁸⁹

⁸⁸ Jf. avsnitt 5.1 og 5.2 (ovenfor).

⁸⁹ Men kan i stor grad være de samme opplysningene.

Slettereglene innebærer at opplysninger vedrørende brukere som ikke har gitt sitt samtykke til trafikkanalyser skal slettes så snart de ikke lenger er nødvendige for de formål som er angitt i ekomforskriften § 7-1 annet ledd (fakturering, trafikkstyring mv). Opplysninger knyttet til brukere som har gitt samtykke til å behandle opplysninger som ledd i trafikkanalyser, kan beholdes/lagres så lenge disse analysene gjør det nødvendig. Informasjon om lagringstid er blant de opplysninger som bør inngå i den informasjonen som gis i forbindelse med innhenting av samtykke.⁹⁰

Kravet til sletting gjelder bokstavelig, dvs. det skal ikke være mulig å reversere prosessen og på den måten gjenskape dataene. Som tidligere understreket kan imidlertid de samme opplysningene samtidig være lagret for et annet formål, men skal da sikres slik at uvedkommende ikke får tilgang. Personer som har hatt tilgang til trafikkdata som ledd i trafikkanalyse, vil derfor i utgangspunktet ikke ha tilgang til trafikkdata som beholdes pga lagringsplikt knyttet til kriminalitetsbekjempelse. I praksis vil det imidlertid lett skje at det er de samme personene som blir autorisert for tilgang til trafikkdata for henholdsvis trafikkanalyse og datalagring for politiformål mv. Årsaken er at mange tjenestetilbydere er så små virksomheter at de samme personene må utføre flere/alle oppgaver knyttet til trafikkdata.

6.4 Oppsummering

Poenget i dette kapittelet er at trafikkdata som anvendes for trafikkanalyse er underlagt taushetsplikt etter ekomloven § 2-9, og skal sikres i samsvar med bestemmelsene i ekomloven §§ 2-7 og 2-9, samt bestemmelsene om sikring av personopplysninger i pol § 13 og personopplysningsforskriftens kapittel 2. Dette innebærer bl.a. krav til gjennomføring av risikoanalyse mv i samsvar med generelle regler. Det er grunn til å tro at risikovurderingen vil komme til å være relativt streng, noe som kan innebære forholdsvis omfattende og dyre sikkerhetstiltak.

⁹⁰ Jf. avsnitt 5.3.2.

7 SPESIELT OM INNSYNSRETT OG INFORMASJONSPLIKT

I ekomloven er det ikke gitt egne bestemmelser om innsynsrett i trafikkdata for brukere. Riktignok må det forutsettes slik informasjonstilgang som er nødvendig for de formål for behandling av trafikkdata som er angitt i loven, jf § 2-7 annet ledd og ekomforskriften § 7-1 annet ledd. Det betyr bl.a. at sluttbruker har innsynsrett i alle data som benyttes for faktureringsformål. Imidlertid er det neppe grunnlag for å utlede noen innsynsrett etter ekomlovgivningen for den som bare er bruker (og altså ikke er sluttbruker/abonnent). For trafikkdata som også er personopplysninger, gjelder imidlertid personopplysningsloven, inkludert denne lovens regler om innsyn for og informasjon til den registrerte (se lovens kapittel III). For disse opplysningene gjelder omfattende innsynsrettigheter.

I avsnitt 4.3.4 konkluderte jeg med at «registrert» i tilknytning til digitale TV-sendinger i alle fall er personer som hører til den husstanden der apparatet står. Det er mulig at kretsen er noe større enn dette, men tilfeldige brukere/gjester i sluttbrukers hushold kan neppe ses som registrert person etter personopplysningsloven.⁹¹ Det er kun registrerte personer som har rett til individuelt innsyn,⁹² og som den behandlingsansvarlige har plikt til å gi opplysninger.⁹³ Personer i husstanden som er mindreårige, kan måtte utøve rettighetene sine ved hjelp av foreldre, jf. diskusjonen vedrørende samtykke (avsnitt 5.3.1). Her kommer jeg imidlertid ikke nærmere inn på de særlige spørsmål som dette reiser.

Bestemmelsene om plikt for den behandlingsansvarlige til å gi registrerte personer informasjon etter §§ 19 og 20, passer dårlig for digital-TV.⁹⁴ Bestemmelsene gjelder plikt til å informere når den behandlingsansvarlige enten innhenter opplysninger fra den registrerte selv (§ 19), eller innhenter opplysninger om den registrerte fra tredjepersoner (§ 20). Skjer det innhenting direkte fra en konkret person i husholdet, er kommunikasjonsforholdet uproblematisk. Trafikkanalyser som er omhandlet i denne rapporten innebærer imidlertid at det kan samles inn opplysninger om en eller flere personer i vedkommende

⁹¹ Se drøftelsene i avsnitt 5.3.1.

⁹² Jf. pol § 18 annet og tredje ledd.

⁹³ Jf. pol §§ 19 og 20.

⁹⁴ Merk at jeg i avsnitt 5.3.2 har anvendt § 19 for å konkretisere hvilke krav til informasjon som stilles i forbindelse med innhenting av samtykke. Dette er et annet spørsmål enn bruk av §§ 19 og 20 direkte.

hushold, men uten at den som samler inn opplysningene konkret vet hvem dette er. Derfor kan den praktiske gjennomføringen av informasjonsplikten by på problemer. Informasjonsplikten faller imidlertid bort dersom «det er på det rene at den registrerte allerede kjenner til informasjonen om hvem som gjør trafikkanalysene, formålet med behandlingen mv.»⁹⁵ Dersom denne informasjonen gis i tilknytning til innhenting av samtykke, faller derfor informasjonsplikten bort, og problemet med å finne rett adressat blir uaktuelt.

Et vilkår for at den enkelte registrerte person kan anvende innsynsretten i individuelle opplysninger, er at vedkommende kan autentiseres på tilstrekkelig måte; dvs. personopplysninger må bare gis til de det faktisk er registrert opplysninger om. Personopplysningsloven § 24 innebærer at opplysninger det er innsynsrett i kan kreves skriftlig hos den behandlingsansvarlige/tjenestetilbyder.⁹⁶ Den behandlingsansvarlige må i så fall forsikre seg om at opplysningene gis til berettigede personer, dvs. en «registrert» som opplysningene gjelder. Nevnte bestemmelse fastsetter at den behandlingsansvarlige kan kreve at «den registrerte leverer en skriftlig og undertegnet begjæring». Bestemmelsen må imidlertid suppleres med de generelle bestemmelsene om informasjonssikkerhet i § 13 og personopplysningsforskriften kapittel 2. Således kan også andre framgangsmåter være tilstrekkelig sikre. Likevel er det neppe anledning til å stille krav til autentisering som er vanskeligere å etterleve enn den rutinen loven direkte beskriver i § 24. Krav til autentisering kan altså neppe brukes for de facto å innskrenke mulighetene for innsyn.

Opplysninger vedrørende trafikkanalyser er knyttet til personer i det aktuelle husholdet. Samtidig er det imidlertid ikke mulig for tjenestetilbyder som gjør analysen å vite hvilke(n) konkret(e) person(er) i husholdet som faktisk har vært bruker og som opplysningene derfor direkte kan knyttes til. Dersom alle personer i husholdet blir regnet som innsynsberettigede «registrerte» personer, vil personer som ber om innsyn i realiteten be om innsyn som gjelder én eller flere andre i husholdet. Samtidig vil det bare være personer i husholdet som kan ha konkret kjennskap til hvilke personer opplysningene faktisk sier noe om. Spørsmålet blir derfor om det er tilstrekkelig at én person krever innsyn, eller om alle personer i husholdet må be om innsyn for på den måten sikre at de er enighet mellom alle personer det kan være opplysninger om?

Dersom det er nok at én person i et hushold der flere myndige personer bor kan be om innsyn i trafikkdata som viser TV-bruk i husholdet, ville det innebære at personer i husholdet i realiteten kan be om opplysninger som vedkom-

95 Se § 19 annet ledd, jf. første ledd.

96 Opplysningene kan også kreves hos den behandlingsansvarliges databehandler, dvs. virksomhet eller enkeltperson som behandler personopplysninger på den behandlingsansvarliges vegne som et avtaleregulert oppdrag, se pol § 2 nr 5, jf § 15.

mende vet bare gjelder en annen. En ektefelle som har vært på reise, kan i så fall for eksempel be om innsyn i TV-bruk som kun gjelder den andre ektefellen og eventuelle barn. En slik innsynsrett ville med andre ord skje på bekostning av andres krav på personvern, og kan derfor neppe være en holdbar forståelse av rettstilstanden. Jeg antar derfor innsynsbegjæringer må være felles for alle myndige personer i husholdet.

Når det gjelder mindreårige familiemedlemmer, kan de neppe sies å ha en selvstendig rett til å kreve innsyn. Barn må derfor trolig kreve innsyn sammen med foreldre. Riktignok skal barn ha stadig større selvbestemmelsesrett etter hvert som de blir eldre og mer modne. Det kan kanskje komme i konflikt med dette dersom foreldre skal kunne kreve innsyn i TV-bruk de vet kun gjelder deres 17-åring uten at ungdommen er enig i innsynet. På den annen side kan det være at et slikt innsyn kan begrunnes i foreldreansvaret også i forhold til så store ungdommer. Dessuten vil det by på store praktiske problemer dersom også visse barn under 18 år skulle ha rett til å kreve innsyn på lik linje med foreldre/sluttbruker. Jeg antar derfor at det er holdbart å hevde at mindreårige bare helt unntaksvis kan ha selvstendig rett til innsyn.

8 AVSLUTTENDE REFLEKSJONER

Denne undersøkelsen av rettslige rammer og vilkår for å gjennomføre trafikkanalyser knyttet til leveranse av digitalt TV, har som hovedkonklusjon at det er rettslig adgang til å gjennomføre slike analyser. Hovedforutsetningen er imidlertid samtykke fra den enkelte bruker. Hvem som faktisk er brukere vil det imidlertid ikke sjelden være vanskelig å få sikker kunnskap om, og uten denne kunnskapen vil det i praksis være store problemer med å innhente samtykke fra aktuelle brukere. Samtykke, som er den eneste muligheten for å skaffe seg rettslig grunnlag som loven åpner for, skaper derfor behov for å identifisere hvem som faktisk er brukere av TV-tjenester. Slik identifisering er neppe formålstjenlig for ivaretagelse av personvern, fordi det innebærer at aktuelle personer må avgi personopplysninger vedrørende TV-bruken. På denne bakgrunn har jeg i avsnittene 5.3.2 og 5.3.3 kort skissert en mulig løsning som kan tilfredsstille krav samtykke samtidig som det ikke skaper behov for identifisering og autentisering av hver enkelt bruker. Ideen er imidlertid uforedlet og må utvikles videre for at det skal kunne gis sikrere svar på om løsningen er rettslig akseptabel.

De rettslige reguleringene jeg har analysert framkommer i et samspill mellom flere regelverk. Særlig er ekomloven med forskrifter og personopplysningsloven med forskrifter viktige. Selv om det er flere saklige sammenhenger mellom disse reguleringene, er ekomloven (som er den nyeste) ikke skrevet spesielt med tanke på relevante bestemmelser i personopplysningsloven. Resultatene fra drøftelser av de generelle sammenhengene mellom de to lovene, er derfor ikke åpenbare og kjente. Kombinasjonen av de to lovene anvendt spesielt på trafikkanalyser av elektronisk kommunikasjon gir i enda mindre grad løsninger som kan sies å være kjente og aksepterte. Selv om det er grunnlag for å trekke konklusjoner om hva som må regnes som gjeldende rett, er det derfor også et spørsmål om denne rettsstilstanden er akseptabel i et *rettspolitisk* perspektiv.

De rettspolitiske vurderingene er særlig aktuelle i forhold til to spørsmålsstillinger: i) er det over hode ønskelig å tillate trafikkanalyser (dvs *selv om* bruker samtykker?), og ii) hvis trafikkanalyser med samtykke bør være tillatt, er eksisterende krav til samtykke forsvarlige og formålstjenlige? Det sist nevnte spørsmålet er for så vidt allerede kommentert i og med skissen til en praktisk samtykke-mekanisme som nevnt ovenfor. Her skal jeg derfor nøye meg med å knytte noen kommentarer til spørsmålet om trafikkanalyser i det hele tatt bør være tillatt selv om brukere har gitt samtykke.

Beskyttelse av privat kommunikasjon er en sentral del av beskyttelsen av privatliv og personopplysninger.⁹⁷ Således beskyttes elektronisk kommunikasjon av straffelovens § 145 annet ledd. I Menneskerettighetsutvalgets forslag til nye grunnlovsbestemmelser for Norge, er det i § 102 foreslått en ordlyd som nettopp understreker dette aspektet: « Enhver har Ret til Respekt for sit Privatliv og Familieliv, sit Hjem og sin Kommunikation.» (min kursiv).⁹⁸ Dersom en er opptatt av å verne om privat kommunikasjon, kan det være grunn til bekymringer for «utglidning» over tid. Således kan det være fare for at det som begynner med tiltak som har relativt begrenset betydning for befolkningen, gradvis får mer omfattende og dyptgripende anvendelse. Det finnes historiske erfaringer som kan sies å bestyrke denne frykten. Således var det på midten av 1970-tallet bare anledning til «telefonavlytting» i saker som gjaldt statens sikkerhet mv og i alvorlige narkotikasaker. I dag er kommunikasjonskontroll og kommunikasjonsavlytting tillatte etterforskningsmidler i en lang rekke alvorlige typer forbrytelser.⁹⁹ En kan på en slik bakgrunn tenke seg en utvikling der trafikkanalyser for det første skjer ut i fra andre behov enn å bedre teknisk kvalitet og brukeropplevelse. For det andre kan en tenke seg analyser som trenger direkte inn i den private sfæren ved å måle opp mot personlig sluttbrukerutstyr (og ikke bare familiens router). For det tredje kan en tenke seg en utvikling der analysene ikke bare gjelder rene trafikkdata, men også beveger seg over grensen for innholdsdata.¹⁰⁰ Med et slikt perspektiv kan spørsmålet om trafikkanalyser bør være tillatt transformeres til et prinsippspørsmål, der en er mer restriktiv enn eksisterende teknologi og intensjoner begrunner.

Det kan uansett spørres om det bør være opp til hver enkelt bruker å samtykke til at trafikkanalyser skal skje. Riktignok er den enkeltes autonomi og rett til å bestemme over opplysninger om egen person en ideologisk grunnstein i lovgivningen om personopplysningsvern. Samtidig er det imidlertid hevdet å være en fare for «samtykketretthet», og for at den enkelte ikke vil ta samtykkesituasjonene på alvor dersom det blir rutine å avgi samtykke i en lang rekke tilfelle. Jo mer rutinisert og trivialisert samtykkerutiner blir, desto mindre betydning kan det hevdes å ha.¹⁰¹ Har samtykke reelt sett liten betydning fordi folk ikke tar

97 Dette kommer bl.a. klart til uttrykk i den tyske grunnlovens artikkel 10 om «telekommunikasjonshemmeligheten». Se nærmere om dette i Mahler m.fl. 2010 s. 154.

98 Se Menneskerettighetsutvalget 2012, s. 180.

99 Se straffeprosessloven kapittel 16a om avlytting og annen kontroll av kommunikasjonsanlegg (kommunikasjonskontroll).

100 For eksempel ved hjelp av «deep packet inspection», jf Read 2010.

101 Jf. Bygrave og Schartum 2009 der forfatterne på denne bakgrunn diskuterer modeller for «kollektivt samtykke».

vurderingene på alvor, kan dette være argument for å velge en «patriarkalsk» tilnærming i stedet, for eksempel ved å velge forskriftsregulering av trafikkanalyser.

9 LITTERATUR OG KILDER

- Blixrud og Ottesen 2010: KB Blixrud og CA Ottesen, Personvern i finanssektoren (Oslo: Gyldendal akademisk, 2010).
- Bygrave & Schartum 2009: LA Bygrave & DW Schartum, «Consent, Proportionality and Collective Power», In Serge Gutwirth; Yves Poullet; Paul De Hert; Cécile de Terwangne & Sjaak Nouwt (ed.), *Reinventing Data Protection?*. Springer Science+Business Media B.V. 2009, kapittel 9, s 157 – 173.
- EU-kommisjonen 2012: Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation).
- Mahler m.fl. 2010: T Mahler, MR Ranheim, & DI Cojocarasu, «Hvordan vurderer nasjonale domstoler datalagringsdirektivet opp mot grunn- og menneskerettigheter?», I: DW Schartum (red.), *Overvåking i en rettsstat*. Fagbokforlaget 2010, kapittel 7, s 149 – 166.
- Menneskerettighetsutvalget 2011, s. 180. Rapport fra Menneskerettighetsutvalget om menneskerettigheter i Grunnloven, avgitt 19. desember 2011 (Stortinget, dokument 16 (2011-2012))
- Read 2012: Darren Read, *Network Neutrality* (Oslo: Norwegian Research Center for Computers and Law, research paper to the project R2D2, 2012). Publisert som del av denne publikasjonen.
- Schartum og Bygrave 2011: DW Schartum og LA Bygrave, *Personvern i informasjonssamfunnet*, (Bergen: Fagbokforlaget, 2011).
- Schartum og Bygrave 2006: DW Schartum og LA Bygrave, *Utredning av behov for endring av personopplysningsloven*, (Oslo: Justisdepartementet, rapport 2006).
- BJ Villa og PE Heegaard: A Monitor Plane Component for Adaptive Video Streaming, paper presented to the NIK-2011 conference.
- Artikkel 29-gruppen 2011: «Opinion 15/2011 on the definition of consent», 13. juli 2011 (01197/11/EN, WP187).

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) – «kommunikasjonsverndirektivet».

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data – «personverndirektivet».

Lov om elektronisk kommunikasjon av 4. juli 2003 nr. 83 (ekomloven).

Forskrift om elektronisk kommunikasjonsnett og elektronisk kommunikasjonstjeneste av 16. februar 2004 nr. 401 (ekomforskriften).

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

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

Lov om barn og foreldre av 8. april 1981 nr. 7 (barnelova).

Lov om rettergangsmåten i straffesaker av 22. mai 1981 nr. 25 (Straffeprosessloven)

NTE: Alminnelige vilkår for avtale om bredbånd mellom privatkunder og NTE.

Innst O nr 51 (1999–2000), Om lov om behandling av personopplysninger (personopplysningsloven).

Ot.prp.nr.92 (1998-1999) Om lov om behandling av personopplysninger (personopplysningsloven).

Ot.prp.nr.58 (2002-2003) Om lov om elektronisk kommunikasjon (ekomloven).

R2D2 Networks: Road to media-aware user-Dependent self-adaptive NETWORKS (R2D2 Networks), prosjektnotat 15. november 2008.

TV2: Avtale- og brukervilkår for tjenester under Tv2.no og andre tjenester levert av eller i samarbeid med TV2 AS hvor TV2 AS er behandlingsansvarlig. (27.10.2011).

Muntlige kilder: Intervju med personer ved NTE (Steinkjer) og TV2 Sumo (Oslo).

TIDLIGERE UTGITT I COMPLEX-SERIEN

CompLex er Senter for rettsinformatikk's skriftserie. Serien startet i 1981, og det har blitt utgitt mer enn hundre titler. Bøkene i CompLex-serien kan bestilles fra Akademika (se bestillingsskjema bak i boken eller www.akademika.no).

2012

- 1/12 Fra kontrollør til aktør: Behov for nye roller for fagdepartementene i styring av tverrgående IKT-prosjekter?
Arild Jansen og Ivar Berg-Jacobsen
IT governance in Norwegian public sector – business as usual?
Arild Jansen and Tommy Tranvik
The functions and roles of ICT in public sector and its impact on management and governance
Arild Jansen NOK xxx,-

2011

- 1/11 Styring av den elektroniske forvaltning i Norge – en tilstandsrapport
Arild Jansen og Ivar Berg-Jacobsen..... NOK 108,-
- 2/11 Tilgang til og videreformidling av helseopplysninger
Herbjørn Andresen NOK 589,50
- 3/11 Automatisert inndragning
Inger Marie Sunde..... NOK 502,50
- 4/11 Senter for rettsinformatikk: Bibliografi 1970-2010
Anne Gunn B. Bekken NOK 327,-
- 5/11 Om avgrensning av arbeidsgivers styringsrett på grunn av arbeidstakers personvern – En gjennomgang av norsk rettspraksis
Mette Borchgrevink NOK 179,-
- 6/11 Legaldefinisjoner i nyere norske lover
Dag Wiese Schartum

Legaldefinisjoner og juridisk interoperabilitet i helsesektoren
Marius Raugstad og Ivar Berg-Jacobsen NOK 299,-

2010

3/10 Extended collective licences – the compatibility of the Nordic
 solution with the international conventions and EC law
Christian Rydning NOK 192,-

2/10 Air Passenger Data Protection – Data Transfer from the European
 Union to the United States
Olga Mironenko NOK 132,-

1/10 Using Citation Analysis Techniques for Computer-Assisted Legal
 Research in Continental Jurisdictions
Anton Geist NOK 210,-

2009

5/09 Anvendelse av straffeloven § 343 hvor det handles
 mot et konvensjonsstridig yringsforbud fastlagt ved
 midlertidig forføyning
Ranveig Tufte Fjerdrumsmoen NOK 87,-

4/09 Personvern og informasjonssikkerhet
Tommy Tranvik NOK 195,-

3/09 Vurdering af PersonVernnemndas Praksis 2001–2008
Peter Blume NOK 852,-

2/09 Legal issues regarding whois databasis
Dana Irina Cojocarasu NOK 258,-

1/09 Åpen programvare – noen rettslige problemstillinger
Odd Randgaard Kleiva NOK 225,-

2008

8/08 Rett og rimelighet i moralsk belysning og andre grunn-
 problemer i norsk rettsliv
Jens Petter Berg NOK 657,-

- 7/08 Vern av tekniske beskyttelsessystemer etter åndsverkslovens §53a
Andreas Norum NOK 156,-
- 6/08 Grunnloven § 100 (4) som hinder for bruk av midlertidige forføyninger mot ytringer – med spesielt fokus på forestående, antatte opphavsrettskrenkelser
Frederik Langeland NOK 132,-
- 5/08 Telekirurgi i et rettslig perspektiv – med spesiell vekt på etikk, samtykke og ansvar
Bjørn Ivar Christie Østberg NOK 201,-
- 4/08 IT-støtte for arbeid med lovsaker
Dag Wiese Schartum NOK 144,-
- 3/08 Juristopia: Semantic Wiki for Legal Information
Ole Christian Rynning NOK 243,-
- 2/08 Electronic Contracting in Europe. Benchmarking of national contract rules of United Kingdom, Germany, Italy and Norway in light of the EU E-commerce Directive
Maryke Silalahi Nuth NOK 192,-
- 1/08 Internet search engines» collecting and processing of web pages – from the perspective of copyright law
Ingvild Jørgensen NOK 165,-

2007

- 5/07 Gjennomgang av arkivretten
Martin Rødland NOK 129,-
- 4/07 Privacy & Identity Management
Thomas Olsen, Tobias Mahler, et al. NOK 234,-
- 3/07 Personvern og transportsikkerhet
Dag Wiese Schartum NOK 306,-
- 2/07 ZEBLEX 06 – Tre avhandlinger om fildeling, IT-sikkerhet og e-postkontroll
*Ida Otterstad, René Stub-Christiansen
& Cecilie Wille Søvik* NOK 348,-

- 1/07 Kontraktsregulering av domstolens kompetanse ved elektronisk handel
Vebjørn Krag Iversen NOK 186,-

2006

- 6/06 Lover – fra kunngjøring til hyperstrukturer: to avhandlinger
Per Marius Slagsvold & Kirill Miazine..... NOK 222,-
- 5/06 Retten til eget bilde
Maria Jongers NOK 198,-
- 4/06 Legal, Privacy, and Security Issues
in Information Technology Vol. 2
Kierkegaard, Sylvia Mercado (editor)..... NOK 783,-
- 3/06 Legal, Privacy, and Security Issues
in Information Technology Vol. 1
Kierkegaard, Sylvia Mercado (editor)..... NOK 918,-
- 2/06 Rettslige reguleringer av informasjonssikkerhet
Are Vegard Haug NOK 420,-
- 1/06 Anti-spam Legislation Between Privacy And
Commercial Interest. An overview of the European
Union legislation regarding the e-mail spam
Dana Irina Cojocarasu..... NOK 155,-

2005

- 1/05 Renessansen som unnfanget Corpus Iuris Civilis.
Keiser Justinians gjenerobring av Romerriket
Halvor Manshaus..... NOK 249,-
- 2/05 Personvern og ytringsfrihet. Fotografering av siktede
i straffesaker – et vern for ytringsfrihet?
Anette Engum..... NOK 132,-
- 3/05 Rettigheter til geografisk informasjon.
Opphavsrett, databasevern og avtalepraksis.
Steinar Taubøll..... NOK 206,-

- 4/05 «The Answer to the Machine is in the Machine»
and Other Collected Writings
Charles Clark.....NOK 401,-
- 5/05 Digital Rights Management – Promises, Problems
and Alternative Solutions
Kristian Syversen.....NOK 201,-
- 6/05 DRM og Demokrati. Argumentasjoner, rettferdiggjøringer
og strategier bak endringen av åndsverksloven 2003–2005
Jan Frode Haugseth NOK 224,-

2004

- 1/04 Opphavsrettslige problemstillinger ved universitetene og høyskolene.
Innstilling fra immaterialrettsutvalget, oppnevnt av Universitets-
og Høgskolerådet 31. januar 2000. Avgitt til universitets- og
høgskolerådet 8. oktober 2003
Immaterialrettsutvalget NOK 341,-
- 2/04 Ansvarsfrihet for formidler ved formidling av
informasjonssamfunnstjenester
Bård Standal NOK 311,-
- 3/04 Arbeidsgivers adgang til å kontrollere og overvåke sine ansatte
med hovedvekt på grunnvilkårene for behandling av
personopplysninger i arbeidslivet
Stefan Jørstad.....NOK 191,-
- 4/04 Elektroniske spor fra mobiltelefoner – om politiets bruk og
teleoperatørenes lagring av trafikkdata.
Christian Dahlgren NOK 117,-
- 5/04 International Jurisdiction and Consumers Contracts – Section 4
of the Brussels Jurisdiction Regulation.
Joakim S. T. Øren NOK 172,50
- 6/04 Elektronisk dokumentfalsk.
Lars Christian Sunde.....NOK 60,502003

2003

- 1/03 IT i domstolene. En analyse av norske domstolars teknologianvendelse fra 1970 til 2001
Even Nerskogen.....NOK 330,-
- 2/03 Hvorfor vokser Norsk Lovtidend? En empirisk analyse av veksten
Martin Støren.....NOK 87,-
- 3/03 Etableringslandsprinsippet. En analyse av e-handelsdirektivet art 3 og prinsippet om fri bevegelighet av tjenester ved elektronisk handel
Jon Christian Thaulow.....NOK 213,-
- 4/03 The Law of Electronic Agents. Legal contributions to ALFEBIITE – A Logical Framework for Ethical Behaviour between Infohabitants in the Information Trading Economy of the Universal Information Ecosystem, IST-1999–10298
Jon Bing and Giovanni Sartor (eds) NOK 351,-
- 5/03 LEA 2003: The Law and Electronic Agents Proceedings of the Second LEA Workshop, 24th June 2003, in connection with the ICAIL 2003 Conference (Ninth International Conference on Artificial Intelligence and Law), Edinburgh, Scotland, UK
Seminarrapport).....NOK 228,-
- 6/03 Opphavsrettslige aspekter ved nettbasert formidling av musikk
Stig Walle NOK 153,-
- 7/03 Sceneinstruktørens opphavsrettslige stilling
Edle Endresen.....NOK 119,-
- 8/03 User-Centred Privacy Aspects In Connection With Location Based Services
Christian B. Hauknes.....NOK 203,-

2002

- 1/02 Koblingshandel og forholdet til fysisk og teknologisk integrasjon i relasjon til EØS-avtalens art.54(d)
Ole Jacob Garder.....NOK 180,-

- 2/02 To opphavsrettslige arbeider:
Bjarte Aambø – Opphavsrettslige rettsmangler
Erlend Ringnes Efskind – Skjermbildets rettslige natur
Aambø / Ringnes Efskind..... NOK 201,-
- 3/02 Arbeidstakeroppfinnelser ved universiteter og høyskoler. Innstilling
fra et utvalg oppnevnt av universitets- og høyskolerådet 31 januar
2000. Avgitt til universitets- og høyskolerådet i oktober 2001
..... NOK 213,-
- 4/02 Utøvende kunstners direkteoverføringer på Internett – med
hovedvekt på kringkastingsbegrepet
Irina Eidsvold Tøien NOK 225,-
- 5/02 Administrasjon av radiofrekvensspekteret. Rettslige problemstillinger
knyttet til telemyndighetenes forvaltning av frekvensressursene
Øyvind Haugen NOK 177,-
- 6/02 Overføring av personopplysninger til tredjeland. Kravet til
tilstrekkelig beskyttelse etter EU-direktivet om personvern art. 25
Mona Naomi Lintvedt og Christopher J. Helgeby..... NOK 198,-
- 7/02 Digitale mellomledds ansvar for videreformidling av ytringer.
E-handelsdirektivet art. 12–14
Just Balstad..... NOK 186,-
- 8/02 Platekontrakten. Eksklusive overdragelser av utøverens rettigheter til
eksemplarframstilling og spredning
Øyvind Berge..... NOK 237,-
- 9/02 Varemerkerettslige konflikter under .no. I hvilken grad kan
registrering og bruk av et domenenavn medføre inngrep i en
varemerkerett? Hvordan løses konflikter under .no i dag, og
hva kan være en mer hensiktsmessig tvisteløsningsmekanisme
i fremtiden?
Silje Johannessen..... NOK 192,-
- 10/02 Vegard Hagen – Pekeransvar. Spørsmålet om ansvar for publisering
av pekere på verdensveven (World Wide Web)
Hans Marius Graasvold – Pekeransvaret. Straffe- og
erstatningsansvar for publisering av pekere til informasjon på
Internett
Vegard Hagen / Martin Grasvold..... NOK 234,-

- 11/02 Personopplysningsloven § 7. En analyse av forholdet mellom personvern og ytringsfrihet slik det er uttrykt i personopplysningsloven § 7
Karen Elise Haug Aronsen.....NOK 198,-

- 12/02 Databasevern. Sui generis-vern av sammenstillinger etter gjennomføringen av databasedirektivet i åndsverkloven § 43
Lisa Vogt Lorentzen.....NOK 210,-

2001

- 1/01 Internet and Choice-of-Law – The International Sale of Digitised Products through the Internet in a European Context
Peter Lenda.....NOK 275,-

- 2/01 Internet Domain Names and Trademarks
Tonje Røste Gulliksen.....NOK 227,-

- 3/01 Internasjonal jurisdiksjon ved elektronisk handel – med Luganokonvensjonen art 5 (5) og elektroniske agenter som eksempel
Joakim S. T. Øren NOK 204,-

- 4/01 Legal issues of maritime virtual organisations
Emily M. Weitzenböck.....NOK 164,-

- 5/01 Cyberspace jurisdiction in the U.S. – The International Dimension of Due Process
Henrik Spang-Hanssen.....NOK 685,-

- 6/01 Norwegian border control in a Europe without Internal Frontiers – Implications for Data Protection and civil liberties
Stephen Kabera Karanja.....NOK 252,-

2000

- 1/00 Klassikervernet i norsk åndsrett
Anne Beth Lange NOK 268,-

- 2/00 Adgangen til å benytte personopplysninger. Med vekt på det opprinnelige behandlingsformålet som begrensningsfaktor
Claude A. Lenth.....NOK 248,-

- 3/00 Innsyn i personopplysninger i elektroniske markedsplasser.
Line Coll...... NOK 148.-

1999

- 1/99 International regulation and protection of Internet domain and
trademarks
Tonje Røste Gulliksen..... NOK 248.-
- 2/99 Betaling via Internett
Camilla Julie Wollan..... NOK 268.-
- 3/99 Internett og jurisdiksjon
Andreas Frølich Fuglesang & Georg Philip Krog..... NOK 198.-

1998

- 1/98 Fotografiske verk og fotografiske bilder, åndsverkloven § 1 og § 43 a
Johan Krabbe-Knudsen..... NOK 198.-
- 2/98 Straffbar hacking, straffelovens § 145 annet ledd
Guru Wanda Wanvik..... NOK 238.-
- 3/98 Interconnection – the obligation to interconnect telecommunications
networks under EC law
Katinka Mahieu..... NOK 198.-

1997

- 1/97 Eksemplarframstilling av litterære verk til privat bruk
Therese Steen..... NOK 158.-
- 2/97 Offentlige anskaffelser av informasjonsteknologi
Camilla Sivesind Tokvam..... NOK 175.-
- 3/97 Rettslige spørsmål knyttet til Oppgaveregisteret
Eiliv Berge Madsen..... NOK 170.-
- 4/97 Private pengespill på Internett
Halvor Manshaus..... NOK 160.-

- 5/97 Normative Structures in Natural and Artificial Systems
Christen Krogh NOK 255.-
- 6/97 Rettslige aspekter ved digital kringkasting
Jon Bing..... NOK 178.-
- 7/97 Elektronisk informasjonsansvar
Tomas Myrbostad NOK 148.-
- 8/97 Avtalelisens etter åndsverksloven § 36
Ingrid Mauritzen..... NOK 120.-
- 9/97 Krav til systemer for forvaltning av immaterielle rettigheter
Svein Engebretsen NOK 168.-
- 10/97 American Telephony: 120 Years on the Road to Full-blown
 Competition
Jason A. Hoida NOK 140.-
- 11/97 Rettslig vern av databaser
Harald Chr Bjelke..... NOK 358.-

1996

- 1/96 Innsynsrett i elektronisk post i offentlig forvaltning
Knut Magnar Aanestad og Tormod S. Johansen..... NOK 218.-
- 2/96 Public Policy and Legal regulation of the Information Market in the
 Digital Network Environment
Stephen John Saxby NOK 238.-
- 3/96 Opplysning på spill
Ellen Lange..... NOK 218.-
- 4/96 Personvern og overføring av personopplysninger til utlandet
Eva I. E. Jarbekk NOK 198.-
- 5/96 Fjernarbeid
Henning Jakhell NOK 235.-
- 6/96 A Legal Advisory System Concerning Electronic Data Interchange
 within the European Community
Andreas Mitrakas..... NOK 128.-

7/96 Elektronisk publisering: Utvalgte rettslige aspekter
Jon Bing og Ole E. Tokvam NOK 186.-

8/96 Fjernsynsovervåking og personvern
Finn-Øyvind H. Langfjell..... NOK 138.-

1995

1/95 Rettslige konsekvenser av digitalisering: Rettighetsadministrasjon og redaktøransvar i digitale nett
Jon Bing..... NOK 368.-

2/95 Rettslige spørsmål i forbindelse med utvikling og bruk av standarder innen telekommunikasjon
Sverre Sandvik NOK 178.-

3/95 Legal Expert Systems: Discussion of Theoretical Assumptions
Tina Smith NOK 278.-

4/95 Personvern og straffeansvar – straffelovens § 390
Ole Tokvam..... NOK 198.-

5/95 Juridisk utredning om filmen «To mistenkelige personer»
Johs. Andenæs NOK 138.-

6/95 Public Administration and Information Technology
Jon Bing and Dag Wiese Schartum NOK 348.-

7/95 Law and Liberty in the Computer Age
Vittorio Frosini NOK 158.-

1994

1/94 Deon'94, Second International Workshop on Deontic Logic in Computer Science
Andrew J. I. Jones & Mark Sergot (ed) NOK 358.-

2/94 Film og videogramrett. TERESA (60)
Beate Jacobsen..... NOK 318.-

3/94 Elektronisk datutveksling i tollforvaltingen – Rettslige spørsmål knyttet til TVINN
Rolf Risnæs..... NOK 225.-

- 4/94 Sykepenger og personvern – Noen problemstillinger knyttet til
behandlingen av sykepenger i Infotrygd
Mari Bø Haugestad.....NOK 148.-
- 5/94 EØS, medier og offentlighet. TERESA (103)
Mads Andenæs, Rolf Høyer og Nils Risvand NOK 148.-
- 6/94 Offentlige informasjonstjenester: Rettslige aspekter
Jon Bing.....NOK148.-
- 7/94 Sattelittfjernsyn og norsk rett. MERETE (3) IV
Nils Eivind Risvand NOK 138.-
- 8/94 Videogram på forespørsel. MERETE (14) IV
Beate Jacobsen (red).....NOK 158.-
- 9/94 «Reverse engineering» av datamaskinprogrammer. TERESA (92) IV
Bjørn Bjerke.....NOK 198.-
- 10/94 Skattemessig behandling av utgifter til anskaffelse av
datamaskinprogrammer. TERESA (75)
Gjert Melsom.....NOK 198.-

1993

- 1/93 Artificial Intelligence and Law. Legal Philosophy and Legal Theory
Giovanni Sartor NOK 148.-
- 2/93 Erstatningsansvar for informasjonstjenester, særlig ved databaseydelser
Connie Smidt NOK 138.-
- 3/93 Personvern i digitale telenett
Ingvild Hanssen-Bauer.....NOK 178.-
- 4/93 Consumers Purchases through Telecommunications in Europe. –
Application of private international law to cross-border contractual
disputes
Joachim Benno.....NOK 198.-
- 5/93 Four essays on: Computers and Information Technology Law
Morten S. Hagedal.....NOK 218.-
- 6/93 Sendetidsfordeling i nærradio MERETE (3) III
Marianne Rytter Evensen.....NOK 148.-

7/93 Essays on Law and Artificial Intelligence
Richard Susskind NOK 158.-

1992

1/92 Avskriving av mikrodatamaskiner med tilbehør – en nordisk studie
TERESA (87)
Beate Hesseltvedt NOK 138.-

2/92 Kringkastingsbegrepet TERESA (78)
Nils Kr. Einstabland NOK 208.-

3/92 Rettskilderegistre i Helsedirektoratet NORIS (94) I & II
Maria Strøm NOK 228.-

4/92 Softwarepatent – Imaterialrettens enfant terrible. En redegjørelse
for patenteringen af softwarerelaterede opfindelser i amerikansk og
europæisk ret
Ditlev Schwanenfügel NOK 158.-

5/92 Abonnementskontrakter fro kabelfjernsyn TERESA (78II)
Lars Borchgrevink Grindal NOK 248.-

6/92 Implementing EDI – a proposal for regulatory form
Rolf Riisnæs NOK 118.-

7/92 Deponering av kildekode»escrow»-klausuler TERESA (79)
Morten S. Hagedal NOK 128.-

8/92 EDB i juridisk undervisning – med en reiserapport fra England og
USA
Ola-Kristian Hoff NOK 228.-

9/92 Universiteters ansvar for bruk av datanett TERESA (94)
Jon Bing & Dag Elgesem NOK 198.-

10/92 Rettslige sider ved teletorg
Andreas Galtung NOK 148.-

BESTILLING

Jeg bestiller herved følgende CompLex-utgivelser:

Number / year: _____
Title: _____
Number / year: _____
Title: _____
Number / year: _____
Title: _____
Number / year: _____
Title: _____
Number / year: _____
Title: _____
Name: _____
Address: _____
Zip code: _____
Telephone number: _____

The reports can be ordered from Akademika:

akademika

Avd. juridisk litteratur Aulabygningen

Karl Johansgt. 47, 0162 Oslo

Telefon: 22 42 54 50

Telefaks: 22 41 17 08

(www.akademika.no) or Unipub (www.unipub.no)