Hvert år oppfordrer vi våre forskere til å gi en artikkel i julegave. Dette er tiende gang Yulex blir sendt ut som vår julehilsen. I år har vi gleden av å presentere ikke mindre enn 7 ph.d-arbeider, og som tidligere år er årets bok blitt en forundringspakke med varierte bidrag. Vi håper at denne pakken vil være til glede.

Every year we ask our researchers to write an article for Christmas. This is the tenth time we send Yulex as a seasonal greeting to our many partners and contacts. This year we proudly present 7 ph.d-theses and as with previous years, the collection of articles covers a wide variety of topics.

- Captain Surveillance v. Mr. X: An Essay on the Semantics and Politics of 'Surveillance Society'
- Hvordan vurderer nasjonale domstoler datalagringsdirektivet opp mot grunn- og menneskerettigheter
- Privacy Regulations on Biometrics in Australia
- Forbindelser mellom risikovurdering og risikohåndtering under et realistisk og et konstruktivistisk perspektiv
- Scenario Study of Biometric Systems at Borders
- Den menneskelige faktor i elektronisk forvaltning
- Informasjonssikkerhet og personvern i skolen
- Da aksjebrevene forsvant
- The lawyer in 2020
- SERI i et bibliografisk perspektiv
- Presentasjon av årets ph.d avhandlinger / ph.d theses 2010

ISBN 978-82-7226-132-9

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

YULEX 2010

2010

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

YULEX 2010

Senter for rettsinformatikk / Avdeling for forvaltningsinformatikk

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

YULEX 2010

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

Henvendelser om denne bok kan gjøres til:

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

ISBN 978-82-7226-132-9
ISSN 0806-1912

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

FORORD

For et fantastisk år 2010 har vært! I dette året var det 40 år siden Jon Bing og Knut S Selmer startet Senter for rettsinformatikk, som det nest første av sitt slag i verden. Feiringen av jubileet knyttet gammelt og nytt sammen, og på festen om kvelden der 150 venner av SERI var samlet, traff veteranene de unge og håpefulle studentene som skal bringe tradisjonene videre.

I den faglige delen av feiringen var oppmerksomheten mest rettet mot aktuell phd-forskning, og vi fikk dermed demonstrert mye av kvaliteten og vekstkraften i miljøet vårt. Nå når jubileumsåret er omme, kan vi telle hele sju doktordisputaser bare i 2010! Stikkord som «legal risk management», «dynamic networks as collaborative contracts», «bioprivacy», «tilgangsstyring til helseopplysninger», «e-commerce contracting», «personvernøkende identitetsforvaltning» og «automatisk inndragning av datafiler» vitner dessuten om en faglig bredde og innovativ tilnærming til forskningsutfordringene. Til slutt i årets Yulex er det tatt inn kortfattede presentasjoner og referanser til hver avhandling. Jeg regner med det blir rift etter disse arbeidene. God lesning!

Til alt hell har 2010 også gitt god uttelling på søknader om forskningsfinansiering. Fire stillinger som postdoktor og flere andre nye prosjekter, bidrar til at vi i 2011 både kan sikre kontinuitet og fornyelse.

Vi har alltid søkt å være et internasjonalt rettet forskningsmiljø. Det er derfor ekstra tilfredsstillende å kunne registrere at fem nasjonaliteter står bak årets avhandlinger. Derfor ønsker vi leserne og alle SERIs venner og kontakter en «Selemat Hari Natal», «Kung His Hsin Nien bing Chu Shen Tan», «IL-Milied It-tajjeb», « Frohe Weihnachten», eller GOD JUL!

Dag Wiese Schartum
Senterleder

FOREWORD

What a fantastic year 2010 has been! This year it has been 40 years since Jon Bing and Knut S. Selmer started the Norwegian Research Center for Computers and Law (NRCCL), which was the first of its kind in the world. Celebration of the jubilee brought the old together with the new, and during the evening event attended by 150 friends of NRCCL, the venerable veterans met the young and promising students who will carry the tradition into the future.

During the more academic portion of the celebration attention was turned to ongoing PhD research, and we were given a demonstration of the strong quality and growth in our academic environment. Now at the end of the jubilee year, we can pride ourselves on a grand total of seven thesis presentations in 2010 alone! Cue words such as «legal risk management», «dynamic networks as collaborative contracts», «bioprivacy», «management of access to health information», «e-commerce contracting», «expanded protective management of identity» and «automatic recovery of files» bear witness to the broad academic range and innovative approaches to the research challenges. Finally, in this year's edition of Yulex, we include a brief presentation and some reference to each thesis. I presume these papers will be in great demand. Good reading!

Fortunately the applications for research funding written in 2010 met with great success. Four post-doctoral fellowship positions and several other new projects will help to ensure continuity and renewal in 2011.

Our goal has always been to be an internationally-oriented research environment. It is therefore an extra pleasure to note that five different nationalities are represented in the theses written this year. Thus, we wish our readers and all of NRCCL's friends and contacts «Selemat Hari Natal», «Kung His Hsin Nien bing Chu Shen Tan», «IL-Milied It-tajjeb», « Frohe Weihnachten», or GOD JUL!

Dag Wiese Schartum
Director of the Center

CONTENTS

CAPTAIN SURVEILLANCE V. MR. X: AN ESSAY ON THE SEMANTICS AND POLITICS OF 'SURVEILLANCE SOCIETY'[1]

Lee A. Bygrave

1 Captain Surveillance v. Mr. X

Behold a boxing ring. Limbering up in one corner is a beefy man with a self-confident air. His training clothes are emblazoned in large, flashy letters with the name «Captain Surveillance». Just underneath the name, and in slightly smaller letters, are the words «You'll never get away». Their ominous import is reinforced by the Captain's physical largesse; indeed, he seems to be gaining bulk by the minute. Around him mill a well-groomed, well-coordinated, well-funded, energetic set of coaches, sparring partners, physiotherapists and doctors. The latter feed the Captain with considerable numbers of tablets taken from mysterious boxes labelled «Carnivore» and «T.I.A.». The only apparent weak point in the Captain's support team is his Public Relations Unit, which tends to be tight-lipped. The spin doctors in that unit are famous for under-communication. Yet they blithely respond to criticism by saying: «Under-communication is the name of the game. We gotta keep those buggers over there guessing.»

Which brings us to the persons in the other corner of the ring—the so-called buggers. Salient in that group is a pale, weedy fellow. He goes by the name of Mr X. He prefers pseudonyms if he cannot be anonymous. He bears two battered boxing gloves: on the one glove is embroidered «privacy», on the other «freedom». Mr. X looks undernourished. Yet he is not alone. Fretting around him is a small, disparate, ragbag bunch of supporters. Many of them look desperate, some look paranoid, but only a few look doomed. In the eyes of most there is a gritty shine that seems to proclaim: «We shall overcome». Or is that gritty shine more the mark of men and women of principle who know that Mr. X will soon be felled for the sake of such principle?

---

1 Text of speech given at the XXIV Nordic Conference on Computers and Law, Oslo, 12 November 2009. The speech has also been published in Dag Wiese Schartum (ed.), *Overvåkning i en rettsstat* (Bergen: Fagbokforlaget, 2010), chapter 2.

Whatever, there is little gritty shine in the eyes of those making up the general audience. They look disinterested and disengaged. Many are yawning; many are wondering if they can get a refund on their ticket—»cos there aint much happenin' in the ring». And the match was, to begin with, scarcely a sell-out. Its existence has hardly registered on the radar screen of the general public. The few who have turned up might have been hoping for a remake of the biblical struggle between David and Goliath. Yet the contestants seem to spend most of their time just shadow boxing or glowering at each other.

The scenario, then, does not look promising in terms of offering a good punch-up. Is it promising, however, as a credible metaphor for the semantics and politics of discourse on the «surveillance society»? Or is it simply a hackneyed, cliché-ridden and disingenuous caricature? In the following, I use the scenario as foil for a brief analysis of discourse on surveillance, focusing on the notion of «surveillance society» as used in the social sciences. I analyse particularly how certain social scientists characterise the meaning, causes and effects of surveillance, and I discuss the political dimensions of their work. My analysis is intended as no more than a sketch. Nonetheless, it is proffered in the belief that it provides a reasonably accurate picture of the main lines of the scholarship in question.

2 The semantics of «surveillance society»

The notion of «surveillance society» is essentially a sociological construct that emerged in the 1980s, primarily in the work of several North American social scientists—Gary T. Marx, Oscar Gandy, David H. Flaherty and, a little later, David Lyon.[2] It has since gained a solid foothold in Europe, most notably in a report for the Information Commissioner of the United Kingdom (UK) published in 2006. The report is authored by the Surveillance Studies Network, which consists of a group of academic researchers hailing predominantly from the field of sociology. The report is titled quite simply «A Report on the Surveillance Society» (hereinafter also termed simply «the report»).[3]

2 See Gary T. Marx, «The Surveillance Society: The Threat of 1984-style techniques», *The Futurist*, 1985, June, pp. 21–6; Oscar Gandy, «The Surveillance Society: Information Technology and Bureaucratic Social Control», *Journal of Communication*, 1989, vol. 39, no. 3, pp. 61–76; David H. Flaherty, *Protecting Privacy in Surveillance Societies* (Chapel Hill: University of North Carolina Press, 1989); David Lyon, *The Electronic Eye: The Rise of Surveillance Society* (Cambridge: Polity Press, 1994).

3 Available at <http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/surveillance_society_full_report_2006.pdf> (last accessed 25 May 2010).

The sociological discourse on «surveillance society» is part of a more general field of scholarship that typically goes under the name of «surveillance studies». It is a productive field with a prodigious amount of literature. It even has its own dedicated electronic journal, *Surveillance and Society*.[4] The field's principal remit is summed up as

> *focusing a spotlight on the ways in which ordinary details of daily life are noted, watched, monitored, recorded, traced and tracked and asking how this happens, who does it to whom, why it is done, how its subjects respond and sometimes resist, what the consequences are and who and what are affected.*[5]

The notion of «surveillance society» features centrally in this scholastic effort. What exactly does it denote? Basically, the notion denotes a society in which surveillance is integral to it. In the words of «A Report on the Surveillance Society», this is a society in which surveillance systems «represent a basic, complex infrastructure which assumes that gathering and processing personal data is vital to contemporary living» (para. 1.2). Such a society, the report claims, is our society:

> *We live in a surveillance society. It is pointless to talk about surveillance society in the future tense. In all the rich countries of the world, everyday life is suffused with surveillance encounters, not merely from dusk to dawn but 24/7 (para. 1.1).*

This claim is in keeping with one of the tenets of contemporary sociology which is that a high level of surveillance is a key defining feature of modernity.[6] As pithily put by the report, «surveillance grows as a part of just being modern» (para. 1.6). Surveillance is understood in this context as essentially the systematic monitoring of persons and personal data with a view to exercising influence or control.[7] To cite the report:

---

4 Available at <http://www.surveillance-and-society.org/ojs/index.php/journal>.

5 David Lyon, *Surveillance Studies: An Overview* (Cambridge: Polity, 2007), p. 197.

6 See, e.g., Anthony Giddens, *The Consequences of Modernity* (Cambridge: Polity Press, 1990), pp. 57–8; David Lyon (n. 1), pp. 3–4.

7 See, e.g., David Lyon, *Surveillance Society: Monitoring Everyday Life* (Buckingham: Open University Press, 2001), p. 2 (defining surveillance as «collection and processing of personal data, whether identifiable or not, for the purposes of influencing or managing those whose data have been garnered»). Note that other terms are sometimes used to highlight particular types of surveillance. The most prominent term in point is «dataveillance», which has been coined by Roger Clarke to denote surveillance carried out by the systematic use of personal

> *Where we find purposeful, routine, systematic and focused attention paid to personal details, for the sake of control, entitlement, management, influence or protection, we are looking at surveillance (para. 3.1).*

Implicit in the tenet that surveillance is integral to modernity is recognition that the level of surveillance has radically increased from pre-modern times, at least with respect to *mass* surveillance (i.e., surveillance of large numbers of persons, either as individuals or as groups). Some sociologists have recognized, though, that growth in mass surveillance has been offset by declining intensity, at least in many Western countries, of surveillance exercised by and within small-scale groups, such as families and neighbourhoods.[8] Yet arguably the latter trend has been recently offset in turn by the growth in numbers of persons who privately possess the technological means to easily capture and disseminate massive amounts of personal information, also in small-scale groups.[9] Thus, all in all, the physical largesse of Captain Surveillance in the opening scenario rings true. Whether his apparently rapid gains in bulk will persist, however, is less certain from a sociological perspective. For example, the authors of «A Report on the Surveillance Society» are careful not to mount bombastic claims about the future. The general tenor of the report suggests, nevertheless, that surveillance levels are highly unlikely to fall, and the vignettes of life in 2016 presented in the report (see Part C/2) depict a broad range of surveillance mechanisms being applied in ways that are significantly more pervasive than those of 2006.

Joined to the sociological tenet that surveillance is integral to modernity is recognition that the increase in surveillance, at least in Western liberal democracies, is not predominantly the result of secret, Machiavellian scheming by powerful elites: «the surveillance society is better thought of as the outcome of modern organizational practices, businesses, government and the military than as a covert conspiracy» (report, para. 1.3). Thus, insofar as Captain Surveillance and his cohorts are supposed to embody nefarious forces, the scenario is inaccurate. Indeed, sociological discourse on the surveillance society recognizes that the aetiology of surveillance is multifaceted. Of causative factors, the report highlights particularly the role played by risk. Building impli-

---

data systems: see, e.g., Roger A. Clarke, «Information Technology and Dataveillance», in Charles Dunlop and Rob Kling (eds.), *Computerization and Controversy* (Boston: Academic Press, 1991), pp. 496–522.

8 See, e.g., James B. Rule, *Private Lives and Public Surveillance* (New York: Schocken Books, 1974), p. 342.

9 A factor that is unfortunately accorded little attention in much of the sociological discourse on surveillance, including the report.

citly on the work of the German sociologist, Ulrich Beck, on «risk society»,[10] the report couples the growth of surveillance to a general increase in risk consciousness and concomitant obsession with safety and security:

> *Surveillance is such a key component of living with risk that it might even be more appropriate to call the surveillance society, the «risk-surveillance society». The response to risk is an emphasis on safety and security. The «risk-surveillance society» has allowed the emergence of a «safety state» obsessed with security and stability (para. 8.2.3).*

Other causative factors highlighted in the report include the role of the military and the growth of private industry dedicated to security (paras. 8.3–8.4) The increasing capacity of individual persons (as opposed to organizations) to capture and disseminate information in their private capacity is also alluded to (para. 8.5.1), though only marginally. One factor that does not come through clearly in the report but is emphasised by other scholars working on the same issues is that surveillance is quite often the result of popular pressure to see justice done in various ways.[11] The purportedly beneficent, distributive logic of the welfare state is a case in point.

Sociological discourse on the surveillance society focuses also on developments in surveillance techniques. While recognizing that these techniques vary considerably from context to context, the general observation is made that they are now automated, de-personalised, capital-intensive operations to a much larger degree than in the past. They are additionally often more physically discreet than their earlier counterparts, and more able to overcome physical barriers, light conditions and limitations of time and space. Hence, the motto «You'll never get away» emblazoned on the training apparel of Captain Surveillance seems apposite.

What the opening scenario does not highlight clearly is that modern surveillance techniques are increasingly aimed at forestalling undesired action rather than operating *ex post facto*.[12] Their pre-emptive character is viewed as a natural consequence of the above-described obsession with security and sa-

10 Ulrich Beck, *Risikogesellschaft. Auf den Weg in eine andere Moderne* (Frankfurt am Main: Suhrkamp, 1986); published in English as *Risk Society: Towards a New Modernity* (London: Sage, 1992).

11 See, e.g., James Rule, Douglas McAdam, Linda Stearns & David Uglow, *The Politics of Privacy: Planning for Personal Data Systems as Powerful Technologies* (New York: Elsevier, 1980), pp. 43, 134.

12 See further, e.g., Gary T. Marx, *Undercover: Police Surveillance in America* (Berkeley: University of California Press, 1988), chapter 10; Lyon (n. 1), chapter 3.

fety. Yet the more important point of concern for the scholars who write about these trends is that increased use of pre-emptive strategies for risk management inevitably places large numbers of people under suspicion, thus undermining trust across society. In the words of the report, «[s]ocial relationships depend on trust and permitting ourselves to undermine it in this way seems like slow social suicide» (para. 2.8.2).

3 The politics of «surveillance society»

So far I have touched on the predominantly semantic and empirical dimensions of the sociological discourse on «surveillance society»—that is, the dimensions which define in relatively value-neutral terms what surveillance is, where and how it is carried out, and its effects. I turn in the following to its predominantly political dimensions. There are at least three such dimensions. The first lies inherent in the semantic and empirical dimensions of the discourse. The terminology in much of that discourse is laden with emotive and normative implications. The very notion of «surveillance» is an example on point. Even though social scientists attempt to define it in a relatively value-neutral manner in the abstract, the notion tends to have negative connotations in practice, at least in broader political discourse. This is partly a legacy of Orwell's *Nineteen Eighty-Four* and other dystopian literature in which mass surveillance is portrayed as a means for severely curtailing civil liberties.

Moreover, as soon as one attempts to discuss the effects of «surveillance», one is obliged to bring in concepts that are strongly associated with civil liberties, such as privacy, autonomy and integrity. Although these concepts also can be defined in a value-neutral way in the abstract, particularly as certain states or conditions of being,[13] they are in practice normatively laden not least because of the positive value that tends to be ascribed to them—i.e., they are states or conditions to which satisfaction is usually attached. Thus, defining and applying such concepts is not merely a dry, academic exercise.

The semantics adopted feed often into an incessant struggle in the broader arenas for thrashing out public policy. That struggle is one for what could be called the rhetorical «high ground». The struggle is especially important when the terminology is not just normatively laden but also vague. We see this with international debates around protection of «privacy» and «personal integrity». These debates frequently revolve around the questions of when privacy interests are properly engaged, when they are properly threatened,

13 See, e.g., the definitions given in Lee A. Bygrave, *Data Protection Law: Approaching Its Rationale, Logic and Limits* (The Hague: Kluwer Law International, 2002), pp. 23–24.

and what properly amounts to «surveillance». Equivalent questions arise in debates in Norway around «personvern» (the central term used in Norwegian discourse on privacy and data protection).[14] They are questions that have reared their head most recently in the controversy surrounding possible transposition into Norwegian law of the European Union (EU) Data Retention Directive.[15] Part of that controversy has revolved around the validity of claims that the Directive itself constitutes a surveillance measure that places the entire Norwegian population under suspicion.[16]

A second and more obvious political dimension to the sociological discourse on «surveillance society»—and to scholarship in the field of surveillance studies generally—lies in their depiction of many of the effects of surveillance as *problematic* in some way or another. A significant part of the discourse consciously warns of the dangers of surveillance. Thus, «A Report on the Surveillance Society» devotes a large chunk of text to the question «what is wrong with a surveillance society?» (section 2), and it elaborates numerous problems with large-scale surveillance systems. Examples include unfair discrimination and social sorting, engenderment of suspicion and distrust, function creep and corruptions of power.

Some of the work in the surveillance studies field has self-avowedly political ambitions. One of the central scholars, David Lyon, writes:

> *Surveillance is amenable to ethical and moral critique and it ought to be politically contested in many contexts. It is, after all, about power and about persons, two things that I care passionately about.*[17]

In another work, Lyon states:

> *At best, surveillance studies helps to dismantle and destabilize taken-for-granted understandings of the needs for, mechanisms and outcomes of contemporary surveillance, with a view to both empowering data-subjects and calling some new forms of categorical governance into serious question.*[18]

14 For further explication of the term (in English), see Bygrave, *ibid.*, pp. 138–139.

15 Directive 2006/24/EC of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC (O.J. L 105, 13 April 2006, pp. 54–63).

16 See, e.g.,Vidar Refvik, «Datalagring er ikke overvåking», *Bergens Tidende*, 17 December 2009, <http://www.bt.no/meninger/kronikk/Datalagring-er-ikke-overvaaking-985954.html> (last accessed 13 June 2010) and comments thereto.

17 Lyon (n. 6), p. 141.

18 Lyon (n. 4), p. 197.

One can see in these sorts of statements not just an ambition to give surveillance studies a mission of critique but also *resistance*—which again reinforces the political dimension of the scholarship. However, the resistance proffered usually does not involve a call for armed struggle. It tends to take far more moderate, cautious forms, such as calls for vigilance, legislative change, and greater use of «privacy impact assessments» supplemented by «surveillance impact assessments».[19]

A third political dimension inheres in the fact that the notion of «surveillance society» (and what it connotes in terms of societal problems) is gradually moving from academic circles and into more general public consciousness about the effects of surveillance, and can accordingly help to generate political debate about the direction in which society is heading. Indeed, the notion has now come to supplement (though not yet supplant) older notions on point, such as «Big Brother» and «1984». Again, «A Report on the Surveillance Society» is testament to this development—and one cause of it. For example, the report was both an important catalyst and a point of departure for the inquiry by the UK House of Lords Select Committee on the Constitution into the «impact of surveillance and data collection upon the privacy of citizens and their relationship with the State».[20] And the UK Information Commissioner has actively used the notion of «surveillance society» in calls for action to counter the dangers of surveillance.[21] This strategy is mirrored across the Atlantic, for instance, by the American Civil Liberties Union (ACLU). Inspired by the Doomsday Clock created in 1947 to warn about the impending perils of nuclear war, ACLU has created a «Surveillance Society Clock» to warn about the impending perils of «a dark future where our every move, our every transaction, our every communication is recorded, compiled, and stored away, ready to be examined and used against us by the authorities whenever they want».[22]

How do the scholars working in the surveillance studies field see the prospects of success in reigning back or slowing down the forces of surveillance? Certainly their analyses of «surveillance society» are infused with awareness of those forces' immensity—aptly embodied in the steroidal bulk of Captain

19 See, e.g., «A Report on the Surveillance Society», section 45.

20 House of Lords, Select Committee on the Constitution, *Surveillance: Citizens and the State*, Second Report of Session 2008–09, HL Paper 18–I (London: HMSO, 2009), particularly paragraphs 4–5, 20–22.

21 See, e.g., «Watchdog's Big Brother UK Warning», BBC News, 16 August 2004, <http://news.bbc.co.uk/2/hi/uk_news/politics/3568468.stm> (last accessed 15 June 2010).

22 See <http://www.aclu.org/technology-and-liberty/surveillance-society-clock-more> (last accessed 15 June 2010).

Surveillance. The counter-struggle and its depiction are accordingly tinged with a sense of urgency and, occasionally, desperation. However, analysis of its prospects is usually not couched in the rhetoric of outright despair—just as the supporters of Mr. X appear not to be devoid of all hope for their cause. The mood of the scholarship is at times pessimistic but the pessimism rarely matches the classic dystopian visions of fiction, where there is darkness at noon (to borrow Koestler's phrasing)[23] and where all paths lead ultimately to room 101 (Orwell). Rather the mood reflects a view of a society in the balance, a society close to the point at which privacy lies with a broken back but not yet at that point. Jim Rule's recent monograph, *Privacy in Peril*, illustrates this well.[24] Although much of the book is devoted to explicating the multiple pressures put on privacy and related interests by mass surveillance, and, indeed, argues that there is no natural limit on many organisations' appetite for personal data, it does not embrace the view that privacy is or must become an anachronism, and it proffers a range of privacy-enhancing options for serious consideration. The authors of «A Report on the Surveillance Society» take a similar line.

The mood of the scholarship is arguably epitomised in the «Surveillance Society Clock» created by ACLU. The clock is set at 23.55. This is close enough to midnight to signal desperation and urgency, yet far enough away from the witching hour to signal hope rather than inevitable doom—and far enough away to still warrant a call for privacy-enhancing action. It bears emphasis, though, that many scholars are reluctant to pinpoint precisely the status of privacy and associated interests relative to the forces of surveillance. This is because the interaction of privacy and associated interests on the one side and surveillance on the other is seen as too complex and multifaceted to draw properly grounded conclusions as to where exactly the balance between each lies. As Colin Bennett notes, «there is no one trajectory by which we can measure the progress or regress of privacy protection at any one time».[25] Or, in the words of Jim Rule, «it would be absurd to suggest that the transition to a world shaped by institutional use of computerized personal data necessarily means a *net* loss for privacy …».[26] Rule goes on to note, for instance,

23 I am referring here to Arthur Koestler's classic, *Darkness at Noon*, first published in 1940.
24 James B. Rule, *Privacy in Peril* (New York: Oxford University Press, 2007).
25 Colin J. Bennett, *The Privacy Advocates: Resisting the Spread of Surveillance* (Cambridge, Mass.: MIT Press, 2008), p. 221. See too Colin J. Bennett and Charles D. Raab, *The Governance of Privacy: Policy Instruments in Global Perspective* (Cambridge, Mass.: MIT Press, 2006), particularly p. 295.
26 Rule (n. 23), p. xi.

how «face-to-face demands on privacy decrease in a world where personal acquaintance matters less».[27]

What do surveillance studies scholars perceive as hindrances in the struggle to check or roll back surveillance? Numerous hindrances are identified—technological, organisational, ideological, economic, legal. Regarding the latter, most scholars are strongly sceptical of the ability of privacy/data protection laws to seriously curb surveillance practices. The general view is that such laws tend not to radically threaten organisations' established systems of surveillance; they simply seek to make these systems more efficient, fair and, hence, socially acceptable. As a result, it is argued, the laws facilitate avoidance of a «frontal collision» between the privacy demands of the general populace and the surveillance practices of organisations.[28]

Yet the more critical hindrance to countering surveillance is typically identified as «the rather mundane fact that the benefits of surveillance are attractive to many, and well promoted».[29] A closely related factor is fickle and superficial concern for privacy on the part of the general public—recall the general disinterest in the bout in the opening scenario. One result is that the cause of counter-surveillance fails to muster a large, well-funded and persistent social movement—recall the small, ragbag support team for Mr. X. In the words of Colin Bennett:

> *There is no concerted worldwide privacy movement that has anything like the scale, resources or public recognition of organizations in the environmental, feminist, consumer protection, and human rights fields. […] When privacy conflicts arise, they tend to be waged by loose coalitions that come together for specific causes and then disband».*[30]

Concomitantly, claims Lyon, «it is unlikely that in the case of resistance to surveillance items like data protection and privacy would ever become political 'hot button' issues …».[31] Thus, Lyon intimates, there is, in a sense, little «politics» regarding the «surveillance society».

27 *Id.*
28 See generally, e.g., Rule *et al.* (n. 10); see too, eg., Lyon (n. 6), p. 137.
29 Lyon (n. 6), p. 136.
30 Bennett (n. 24), p. 199.
31 Lyon (n. 6), p. 135.

4 The challenges of the boxing ring

In the final part of this essay, I want to raise some critical questions about the quality of scholarship in the field of surveillance studies and, more importantly, about its interaction with broader arenas for elaborating public policy. These questions include: how self-referential is the scholarship? How diverse are its sources of input? How much does it attempt to engage with other academic disciplines? How much does it attempt to engage with wider policy and regulatory discourses? In my opinion, these questions are particularly pertinent in light of the political ambitions of much of the scholarship. I am not sufficiently expert in all of the work concerned to provide firm answers to these questions but I have some tentative impressions on point.

First, it seems to me that the surveillance studies field is dominated by sociologists and political scientists, with a smattering of legal scholars on the margins. I am struck by the apparent absence of economists. That absence is unfortunate as economists could likely contribute usefully to analysis of the costs and benefits of surveillance measures. It is also unfortunate that so few legal scholars are engaged in the field as a great deal of mass surveillance is mediated, facilitated and regulated by law. Moreover, legal scholarship could help to provide a bridge between the academic arena and arenas in which formal regulatory policy is drafted.

A second impression is that the notion of the «panopticon» as first elaborated by the renowned French sociologist, Michel Foucault, on the basis of Jeremy Bentham's prison plan of 1791,[32] has been, and remains central in the discourse of the field. Indeed, one could be forgiven for concluding that the discourse occurs largely within its own panopticon-like structure, where Foucault sits in the central watch-tower and his disciples sit in each of the surrounding cells. The centrality of the panopticon has not gone without criticism from within the field itself. Thus, the Canadian sociologist, Kevin Haggerty, himself a prominent surveillance studies scholar, complains that «[t]he panopticon is oppressive» because it is the «leading scholarly model or metaphor for analysing surveillance» and has become «reified».[33]

32 Michel Foucault, *Discipline and Punish: The Birth of the Prison*, trans A Sheridan (Harmondsworth: Penguin, 1977), pp. 195–228. Bentham's plan was for the building of a prison he termed the Panopticon. The prison would allow for the constant surveillance of prisoners from a central watch tower but prevent (through special lighting devices) prisoners from identifying when and by whom they were watched.

33 Kevin D. Haggerty, «Tear down the walls: on demolishing the panopticon», in David Lyon (ed.), *Theorizing Surveillance: The Panopticon and Beyond* (Cullompton, Devon: Willan Publishing, 2006), p. 23.

A third impression, closely linked to the second, is that there is a tendency within the field to cultivate the abstract and to do so in a self-contained, self-referential manner. Indeed, many in the field seem preoccupied with showing how deftly they can leap between the conceptual and theoretical trapezes hung by certain French scholars, such as Foucault, Jean Baudrillard and Gilles Deleuze. It seems almost the case that one's credentials in the field are established by showing expertise in the work of such scholars. While the fact that considerable parts of their work are difficult to comprehend might add prestige to these «rites of passage», it hardly furthers the ability to communicate usefully within broader public policy discourses. Even the writings of David Lyon, who comes across as one of the most pragmatic and «down-to-earth» scholars in the field, are often rather rarefied, particularly when attempting to offer «new» approaches or perspectives.[34]

That shortcoming is very unfortunate because the broader public policy discourses already have a rather surreal quality. There is, to return to the opening scenario, a great deal of shadow boxing. Much of the public discourse on surveillance issues is couched in terms of potential threats rather than actual threats. Unsupported claims and assumptions are frequently made. There is a need for more documentation based on concrete, empirically based risk assessment. We see this especially in relation to the push for the adoption and implementation of the Data Retention Directive where there is a paucity of published, comprehensive assessment of the costs and benefits involved.[35] We see it too in relation to the incipient rollout of new body-scanning devices at airports.[36]

Hence, in metaphorical terms, it would be desirable to see the physical muscle of Captain Surveillance become more proportionate to the efforts made in documenting the apparent need for his punch. The tight-lipped nature of his Public Relations Unit does little to meet this call for documentation. Yet if the academic supporters of Mr. X are going to help bring real pressure to bear on the Captain and his crew to put more effort into producing proper documentation, they must hone their message so that it has force in the boxing ring.

---

34 See, e.g., Lyon (n. 6), pp. 151–154 (writing about the need to «re-embody persons»).

35 See further, e.g., «Individ og integritet» [Individual and integrity], *Norges Offentlige Utredninger* [Official Reports to the Norwegian Government], 2009: 1, p. 197 (referring to the lack of comprehensive cost-benefit studies prior to the introduction of surveillance measures, particularly in the transport and communications sectors).

36 See, e.g., European Parliament, «Resolution on the impact of aviation security measures and body scanners on human rights, privacy, personal dignity and data protection» (23 October 2008) P6_TA-PROV(2008)0521 (criticising the European Commission for proposing the introduction of such devices without first carrying out systematic assessments of their impact on fundamental rights and public health).

In general, discourse in the field of surveillance studies is one of fine distinctions and subtle nuances, much of it directed at complex, theoretical constructs, much of it couched in a nebulous jargon. Such characteristics are far from unique for surveillance studies; they apply across most if not all of the social sciences. And they are reinforced by the rules of academia which tend to prize appreciation of shades of grey over black and white, and construction or deconstruction of sophisticated theoretical frameworks. Yet such appreciation and focus frequently fail to deliver much punch in the boxing rings in which public policy is fought and forged.

Certainly there are laudatory attempts by surveillance studies scholars to break out and engage with wider policy and regulatory discourses, using language largely stripped of «in-house» jargon. The report for the UK Information Commissioner is probably the most salient example on point. Nonetheless, such attempts are too few and far between. For the most part, the surveillance studies field remains effectively an ivory-tower discourse that rarely if ever escapes the boundaries of its walls or—in the imagery of its beloved panopticon—the walls of the surrounding cells. The result is a poorer politics of surveillance society.

HVORDAN VURDERER NASJONALE DOMSTOLER DATALAGRINGSDIREKTIVET OPP MOT GRUNN- OG MENNESKERETTIGHETER?[1]

Tobias Mahler, Malin Renate Ranheim og Dana Irina Cojocarasu

1 Innledning

Datalagringsdirektivet[2] har vært omdiskutert helt siden det første forslaget ble fremmet. Et sentralt punkt for direktivets motstandere er at det strider mot menneskerettighetene i den europeiske menneskerettighetskonvensjonen (EMK) og respektive grunnrettighetskataloger i nasjonale forfatninger.[3] I skrivende stund[4] er direktivets fremtid åpen. EU skal evaluere direktivet, og mens noen land fortsatt diskuterer om og eventuelt hvordan direktivet skal gjennomføres, har andre land allerede fått prøvd sine datalagringslover for domstolene. På nåværende tidspunkt har verken den europeiske menneskerettighetsdomstolen i Strasbourg, (EMD) eller EU domstolen i Luxemburg, (EUD) tatt stilling til om direktivet eller datalagringslovene strider mot menneskerettighetene.[5]

Denne artikkelen omhandler tre dommer fra henholdsvis Bulgaria, Romania og Tyskland, som alle har erklært de respektive nasjonale lovene for grunnlovsstridige. [6] Vi er ikke kjent med saker der datalagringslover har blitt prøvet uten at den respektive domstolen har funnet brudd med menneskerettighetene. Til tross for at domstolenes argumentasjon kretser rundt direktivets gjennomføring i nasjonalt rett, har de fleste av argumentene i disse dommene en overføringsverdi på flere plan. For det første kan de brukes som en veiledning for eventuelt å gjennomføre direktivet på en måte som ikke strider mot menneskerettighetene. Dette forutsetter imidlertid at man, som i den tyske

1 Artikkelen er opprinnelig publisert i Dag Wiese Schartum (red.), *Overvåkning i en rettsstat* (Bergen: Fagbokforlaget, 2010)
2 Direktiv 2006/24/EF, heretter også omtalt som «direktivet».
3 For tyske referanser til denne diskusjonen se den BVerfG, 1BvR 256/08 av 02.03.2010, avsnitt 82.
4 Juli 2010.
5 I sak C-301/06, Irland vs. Parliament and Council, har EUD kun tatt stilling til kompetansespørsmål.
6 Hovedfokuset vil være de to sistnevnte avgjørelsene, fordi den bulgarske dommen ikke er oversatt.

dommen, mener at det i det hele tatt er mulig å gjennomføre direktivet uten å krenke retten til privatliv etter EMK art 8. Alternativt kan argumentene i dommene få betydning dersom andre lands datalagringslover blir et tema ved en nasjonal eller europeisk domstol. Og for det tredje vil EUs evaluering av direktivet også måtte ta stilling til hvorvidt direktivets virkeområde bør utvides for å inkludere teknologier og bruksmåter (for eksempel sosiale medier) som per i dag ikke er direkte omfattet av lagringsplikten.[7] På denne bakgrunn mener vi det er av interesse å sammenligne de sentrale argumentene fra de tre dommene og analysere overføringsverdien, bl.a. i lys av EMDs rettspraksis.

Den videre fremstillingen er strukturert som følger: Innledningsvis introduserer vi direktivet og datalagringslovene i de tre landene. Deretter beskriver vi rettskildene og de viktigste prinsippene domstolene har benyttet når de vurderte datalagringens grunnlovsmessighet. Innenfor EMK fremkommer disse kriteriene av de generelle skrankene for inngrep i personvernet (etter EMK art 8). Domstolene drøfter særlig proporsjonalitetsprinsippet, beskyttelse av kjernen av rettigheten og krav til klare lovhjemler. Særlig den tyske dommen stiller meget strenge krav til datasikkerhet, til utlevering og bruk av data, til transparens og til rettsvern mot urettmessig bruk av data. Dommene inneholder også en del detaljer som fortjener å bli løftet opp i den europeiske debatten, herunder særskilte regler om IP adresseopplysninger, ulike løsninger for myndighetenes tilgang til data, etterretningens databruk og vern av anonymitet i bestemte relasjoner. Avslutningsvis sammenfatter vi de viktigste argumentene som har kommet frem i dommene.

2 Datalagringsdirektivet og nasjonale datalagringslover

Dommene må forstås i lys av bestemmelsene i datalagringsdirektivet og de ulike løsningene som ble valgt for å gjennomføre det i tysk, rumensk og bulgarsk rett. For enkelthetens skyld bruker vi her samlebegrepet «datalagringslov» om de nasjonale lovene, uten hensyn til om en tilsvarende betegnelse brukes i det respektive landet.

Datalagringsdirektivets kjerne består av følgende to regler: For det første pålegges statene å innføre en generell *lagringsplikt* i 6 - 24 måneder for bestemte typer data (art 3, 5 og 6). Både Romania og Tyskland hadde valgt den kortest mulige lagringstiden på 6 måneder.[8] For det andre krever direktivets art 4 at lagret data «*kun udleveres til de kompetente nationale myndigheder i særli-*

7 Se for eksempel EU Parlamentets «Written declaration on setting up a European early warning system (EWS) for paedophiles and sex offenders 29/2010», 19. april 2010.

8 § 113a i den tyske Teleloven (TKG) og § 3 (2) i den rumenske loven.

ge sager og i overensstemmelse med national lovgivning.» Datalagringslovene i Romania og Tyskland ga bestemte myndigheter en *kompetanse* til å kreve de lagrede data utlevert, samtidig som tjenestetilbyderne ble underlagt en *plikt* til å utlevere disse.

Datalagringsdirektivet ble innført i rumensk rett gjennom en datalagringslov[9] samt en rekke endringer i den eksisterende loven om personvern i elektronisk kommunikasjon.[10] I følge den rumenske datalagringslovens § 16 kunne anmodningen om utlevering fremmes i henhold til reglene i straffeprosessloven. Dette forutsatte at det var reist tiltale[11] i en straffesak etter konkret mistanke om at alvorlig kriminalitet[12] var planlagt eller begått. Domstolens begrunnede godkjenning måtte som hovedregel foreligge før tiltaket kunne igangsettes. [13] Nasjonale sikkerhetsmyndigheter kunne dessuten få tilgang til lagrede data i henhold til lovbestemmelsene som regulerer deres aktivitet. [14]

Tyskland hadde gjennomført direktivet slikt at lagrede data kunne utleveres under visse forutsetninger og for visse formål.[15] Tillatte formål var (i) straffeforfølgning (ii) forebygning mot særlige farer mot den offentlige sikkerhet, eller (iii) for å tjene etterretningstjenestenes lovlige oppgaver. Lovlig utlevering krevde imidlertid *i tillegg* at utleveringen var regulert i en annen lovbestemmelse. Et sentralt eksempel på en slik lov er straffeprosessloven[16] som tillot innhenting av lagret data dersom bestemte fakta begrunnet mistanke om en straffbar handling. Myndighetene kunne som hovedregel bare innhente data hvis det var mistanke om en straffbar handling av alvorlig betydning – også i det konkrete tilfellet. Henvisningen til det konkrete tilfellet skulle utelukke databruk der den straffbare handlingen falt inn under et alvorlig straffebud uten at selve handlingen var tilstrekkelig alvorlig. For straffbare handlinger begått ved hjelp av telekommunikasjon krevdes det imidlertid ikke at den straffbare handlingen måtte være av alvorlig betydning.

9 Rumensk Lov 298/2008 vedrørende lagring av data som er generert eller bearbeidet av kommunikasjonstjenesteytere til publikum eller av eiere av offentlige kommunikasjonsnettverk.

10 Rumensk Lov 506/2004 vedrørende behandling av personopplysninger og personvern i elektronisk kommunikasjon.

11 Oversettelsen av begreper den rumenske straffeprosessloven brukes uten at forfatterne har undersøkt nærmere om de ulike prosessuelle etappene i norsk rett er ellers sammenlignbare.

12 Begrepet « *alvorlig kriminalitet*» er definert i lovens § 2 første ledd bokstav f og omfatter organisert kriminalitet, terrorisme og kriminalitet rettet mot Romanias grunnleggende nasjonale interesser og statens sikkerhet.

13 Artikkel 15 jf. artikkel 16 i den rumenske datalagringsloven.

14 Artikkel 20 i den rumenske datalagringsloven.

15 § 113 b TKG.

16 § 100 g i den tyske straffeprosessloven (StPO).

Vi har begrenset informasjon om den bulgarske loven, fordi dommen ikke er oversatt til andre språk, men kun løst omtalt på Internett.[17] I mangel av mer pålitelige kilder baserer vi oss heretter på slike fremstillinger. Et av de viktigste særtrekkene ved den bulgarske datalagringen synes å være at myndighetene hadde direkte tilgang til sentralt lagrede data.

3 Tre dommer om datalagringsdirektivet

De tre avgjørelser fra hhv. Bulgaria, Romania og Tyskland gjelder datalagringslovenes grunnlovsmessighet. Domstolenes vurdering er basert på en blanding av elementer fra EMK og nasjonale rettighetskataloger i de respektive forfatningene.

Den første forfatningsrettslige dommen over en datalagringslov basert på direktivet ser ut til å ha kommet fra Bulgaria. Den øverste forvaltningsdomstolen i Bulgaria avsa i 2008 en dom som annullerte lovbestemmelsen som ga myndighetene tilgang til lagret data.[18] Domstolen anså følgende forhold som en krenkelse av retten til privatliv: For det første fastsatte ikke loven tilstrekkelige vilkår og grenser for myndighetenes direkte tilgang til data. For det andre var myndighetenes tilgang ikke underlagt rettslig avgjørelse i forkant av datainnhentingen. Og for det tredje manglet det lovpålagte sikkerhetsmekanismer for å hindre misbruk. Samlet sett anså domstolen vilkårene for databruken for utilstrekkelige og uklare. Retten fant at datalagringsloven representerte et inngrep i retten til privatliv som ikke var forenlig med den bulgarske konstitusjon og EMK.

Den rumenske forfatningsdomstolen traff sin avgjørelse i 2009.[19] Domstolen konkluderte med at loven i sin helhet var grunnlovstridig. Selve plikten til datalagring ble så omfattende at den stred mot proporsjonalitetsprinsippet. Dessuten var reglene om datalagring og databruk på flere punkter for uklare og for vidtgående.

Den tyske forfatningsdomstolens avgjørelse, som ble fattet i 2010, slår fast at den tyske datalagringsloven strider mot grunnlovens vern av hemmelig

17 Se http://www.edri.org/edri-gram/number6.24/bulgarian-administrative-case-data-retention.. Vi har ikke kunnet verifisere om innholdet i dommen er riktig gjengitt.

18 Bulgarias Øverste Forvaltningsdomstol ('Върховния административен съд'), dom 13627, 11. desember 2008. Original tekst: http://www.econ.bg/law86421/enactments/article153902.html.

19 Romania Constitutional Court, decision no. 1258, 8. Oktober 2009. Et utdrag av dommen på norsk er publisert i Lov&Data nr. 101 - mars 2010, s. 23. En uoffisiell engelsk oversettelse er tilgjengelig på http://www.legi-internet.ro/fileadmin/editor_folder/pdf/decision-constitutional-court-romania-data-retention.pdf.

telekommunikasjon.[20] I motsetning til Romania ble den generelle plikten til lagring av telekommunikasjonstrafikkdata *ikke* i seg selv ansett som uforenlig med grunnloven. Dommen stiller imidlertid, basert på proporsjonalitetsprinsippet, strenge krav til datalagringen og databruken. Den krever for det første tilstrekkelig klare regler for å oppnå høy datasikkerhet. For det andre stiller dommen strenge krav til myndighetenes bruk av data og til innbyggernes rettsvern. Dessuten krever dommen transparens om myndighetenes databruk.

På ett sentralt punkt er den tyske dommen mindre streng enn den rumenske: den slår fast at det er mulig å gjennomføre direktivet uten at det kommer i strid med menneskerettighetene. Datalagringsplikten som sådan er ifølge den tyske dommen ikke i strid med grunnloven, forutsatt at datasikkerheten og rettssikkerheten er ivaretatt. Den rumenske dommen sier derimot at selve lagringsplikten i den rumenske loven er grunnlovsstridig. Dermed er det vanskelig å se hvordan direktivet vil kunne gjennomføres i rumensk rett, fordi datalagringsplikten er selve kjernen i direktivet. Dette er et helt sentralt punkt, også i forhold til det foreløpig åpne spørsmålet om direktivet som sådan strider mot EMK.

4 Retten til privatliv og korrespondanse

Datalagringsdirektivet fortale påpeker at datalagringen må overholde EMK art 8. Dessuten må prosedyrene for adgang til å bruke lagret data fastsettes «*i overensstemmelse med kravet om nødvendighed og proportionalitet, under hensyn til de relevante bestemmelser i EU-retten og folkeretten, herunder navnlig den europæiske menneskerettighedskonvention*» (direktivets art 4 annen setning, vår kursiv).

EMK art 8 verner om retten til privatliv, herunder enkeltpersoners respekt for sin korrespondanse. Bestemmelsens første ledd angir hva som er vernet («*the right to respect for his private and family life, his home and his correspondence*»), og andre ledd oppstiller vilkår for lovlige inngrep i rettigheten. Datalagringen og databruken vil være et inngrep i retten til privatliv eller korrespondanse etter første ledd. Vurderingen som må foretas under EMK art 8 annet ledd er hvorvidt inngrepet er nødvendig i et demokratisk samfunn av hensyn til, blant annet, den nasjonale sikkerhet og kriminalitetsbekjempelse. Dessuten må kravet til lovhjemmel være oppfylt.

20 BVerfG, 1BvR 256/08 av 02. mars 2010. En sammenfatning av dommen på norsk er publisert i Lov&Data nr. 102 - juni 2010, s. 19-23.

Den rumenske og den bulgarske dommen er fattet både på bakgrunn av EMK og de respektive forfatningsbestemmelsene.[21] Derimot er den tyske dommen utelukkende basert på nasjonal rett. Den tyske grunnlovens beskyttelse av telekommunikasjonshemmelighet (art 10) sikrer at telekommunikasjon skal kunne foregå uten myndighetenes innsyn. Bestemmelsen fortolkes slik at dette ikke bare gjelder i forhold til kommunikasjonens innhold, men også dens omstendigheter (deltakere, tid, lokasjonsdata osv.). Telekommunikasjonshemmeligheten anses i tysk rett å være *lex specialis* i forhold til grunnlovens rett til personvern («Recht auf informationelle Selbstbestimmung»).[22] Det er mulig at ikke alle vurderingene i den tyske dommen ville bli opprettholdt om saken hadde blitt avgjort av EMD. Men forskjellene mellom den tyske grunnlovens art 10 og EMK art 8 virker ikke tilstrekkelig store til å skulle tilsi et strengere rettsvern i tysk rett. Retten til personvern eller hemmelig kommunikasjon/korrespondanse må uansett avveies mot andre hensyn, slik som samfunnets vern mot kriminalitet. Dette følger av proporsjonalitetsprinsippet.

5 Proporsjonalitet

Proporsjonalitetsprinsippet[23] er ulikt behandlet i dommene. Den rumenske dommen fremhever generelt at statens inngrep i retten til privatliv og kommunikasjonshemmeligheten må oppfylle kravene i EMK art 8 og den rumenske grunnlovens art 53, herunder legitimitet, nødvendighet og proporsjonalitet. Basert på dette inneholder den rumenske dommen en avveining av interessene i straffeforfølgning på den ene siden, og interessen i personvern på den andre. Inngrepet i personvernet kunne oppstå ved lagring av data, uten at staten kan vise til årsakssammenheng og andre rettssikkerhetsgarantier som er vanligvis påkrevet i strafferetten og uten at tiltaket kan bringes til opphør når tiltakets medførende årsak faller bort. Domstolen poengterer i tillegg at man ikke bare lagret data knyttet til avsendere, men også om mottakere av meldinger. Datalagringen og bruken av data innskrenker ikke bare den aktive kommunikasjonspartens personvern (dvs. oppringeren eller avsenderen), men også den passive deltakeren. Argumentet var at den passive parten (mottakeren) blir underlagt straffeprosessuelle tiltak uten nødvendigvis å ha vært aktiv i å begå

21 Retten til privat og familieliv er garantert i artikkel 26 i den rumenske grunnloven. Kommunikasjonshemmeligheten garanteres, jf. artikkel 28.

22 «Rettigheten til informasjonell selvbestemmelse». Denne rettigheten utledes av den tyske grunnlovens art 2 annet ledd, første setning i forbindelse med art 1 første ledd.

23 EMD fortolker proporsjonalitetsprinsippet inn i EMK art 8 annet ledd, se S. and Marper v. the United Kingdom (App. 30562/04 og 30566/04) 4. desember 2008, § 101.

terrorisme eller annen alvorlig kriminalitet. På bakgrunn av disse argumentene, konkluderte domstolen med at selve datalagringen var uforholdsmessig.

Dersom man følger dette argumentet, virker det som om det ikke vil være mulig for Romania å gjennomføre direktivet, fordi lagring av mottakerinformasjon er påkrevet etter direktivet. Dette resultatet var antagelig ønsket, i og med at domstolen ikke anser selve datalagringen som proporsjonal. Spørsmålet om lagring av mottakerinformasjon virker etter vårt syn imidlertid lite relevant i denne sammenhengen. Til forskjell fra for eksempel telefonavlytting, der et vesentlig skille går mellom den som er overvåket og tredjepersoner, handler direktivet om lagring av trafikk og lokasjonsdata av alle brukere. Derved blir skillet mellom oppringeren og mottakeren noe kunstig.[24]

Den rumenske dommen avviker både i form og innhold fra den tyske domstolens vurdering av proporsjonalitetsprinsippet. Som nevnt mener den tyske domstolen at plikten til å lagre alles telekommunikasjonsdata ikke nødvendigvis strider mot proporsjonaliteten. Dessuten er den tyske vurderingen av proporsjonalitetsprinsippet betydelig mer formalisert: Domstolen slår først fast at datalagringen og databruken griper inn i retten til hemmelig telekommunikasjon. Deretter vurderer den om inngrepet er rettmessig, noe som fordrer at inngrepet er (i) egnet for å tjene et legitimt formål, (ii) nødvendig og (iii) proporsjonalt etter en interesseavveining.

Den tyske domstolen er ikke i tvil om at datalagringen og bruken av data er egnet for å tjene de legitime formålene straffeforfølgning, forebygging av farer og etterretningens lovlige oppgaver. Inngrepet var også nødvendig, fordi det ikke forelå alternative virkemidler som var mindre inngripende. Av særlig betydning er at metoden «quick freezing», der data blir lagret ved konkret mistanke, ikke er mulig når de data som er interessante for saken allerede er slettet. Den rumenske domstolen derimot legger vekt på at det rumenske lovverket allerede har en bestemmelse for «quick freezing», dvs. audio- og videoopptak og lagring av etterforskningsrelevant kommunikasjonsdata, fastsatt i straffeprosesslovens § 91, og at denne bestemmelsen har i en tidligere domsavsigelse i forfatningsdomstolen, har vært vurdert for å være i henhold til grunnloven.

Den tyske domstolen konsentrerte seg om interesseavveiningen, som blant annet innebærer en vurdering av ulemper og fordeler ved tiltakene. Ulempene er mange: Det fremheves at lagringen anses som et særdeles tungtveiende inngrep, fordi den omfatter så mange personer og deres telekommunikasjonstrafikkdata gjennom seks måneder. Datalagringen var så omfattende at det hadde vært mulig å generere person- og bevegelsesprofiler av nærmest enhver borger. Særlig problematisk var dessuten at data ble lagret uavhengig av om den

24 Se nærmere nedenfor, avsnitt 7.

enkelte foretar en straffbar eller farlig handling. De registrerte ble utsatt for mulig etterforskning, uten å ha gitt noen relevant grunn til dette. For å bli registrert var det for eksempel tilstrekkelig at en person oppholdt seg på et bestemt sted med en mobiltelefon.

Til tross for dette ble datalagringen ikke uten videre ansett som forbudt etter den tyske grunnloven. Domstolen mener at datalagring kan gjøres proporsjonal, hvis man stiller meget strenge krav til *hvordan* data lagres og brukes. Domstolen fremhever imidlertid at datalagringen ikke griper inn i kjernen av retten til «hemmelig» telekommunikasjon. Dette behandles i neste avsnitt.

6 Beskyttelse av kjernen i rettigheten

Etter den tyske grunnloven art 19 II er det forbudt å gripe inn i kjernen av en grunnrettighet. Dette er et separat kriterium som setter noen ytre grenser for hva som kan vurderes under proporsjonalitetsprinsippet. Kriteriet ligner til en viss grad på den ytre grensen EMD setter for bruken av proporsjonalitetsprinsippet.[25]

Den tyske dommen anser at bestemmelsene ikke griper inn i kjernen av telekommunikasjonshemmeligheten. Argumentet er at datalagringsbestemmelsene ikke fører til en fullstendig registrering av kommunikasjon, noe som ville ha vært forbudt. De tyske bestemmelsene ble under tvil ansett som en reaksjon mot kriminalitet. Men domstolen påpeker at lovgivningen ikke må utvikles i retning av mest mulig omfattende lagring av data uten foranledning. Slik lagring må være et unntak.

På dette punktet er som nevnt vurderingene i den tyske og den rumenske dommen forskjellige. Den rumenske domstolen konkluderer med at den vedvarende lagringsplikten er grunnlovstridig, fordi den har et slikt omfang at kjernen av de personlige frihetene i praksis blir tilintetgjort. Domstolen trekker frem avgjørelsen i Prins Hans-Adam II av Liechtenstein mot Tyskland,[26] hvor EMD poengterte at frihetene i EMK skal beskyttes slik at de forblir konkrete og kraftige og ikke bare teoretiske og illusoriske. Her legger den rumenske domstolen vekt på at alle borgerne som bruker vanlige kommunikasjonsmidler omfattes av loven, kontinuerlig, uten at offentlige og private personer skal kunne opptre fritt og uten selvsensur. I denne sammenhengen diskuteres også uskyldspresumsjonen.

25 Se f.eks. S. and Marper v. The United Kingdom, (fotnote17, ovenfor) § 102, med videre henvisninger til tidligere praksis fra EMD.

26 Prins Hans-Adam II av Liechtenstein v. Germany (App. 42527/98) 12. juli 2001.

7 Uskyldspresumsjonen

Både den rumenske og den tyske dommen bruker argumenter som kan knyttes til uskyldspresumsjonen, dvs. retten til å bli ansett som uskyldig inntil det motsatte er bevist. I den rumenske dommen vektlegges det at inngrepet i personvernet oppstår uten at staten kan vise til årsakssammenheng eller andre grunnleggende prinsipper innen strafferetten. Dette diskuteres i sammenheng med proporsjonalitetsprinsippet, men den underliggende vurderingen er knyttet til uskyldspresumpsjonen.

Også den tyske dommen nevner kriterier som peker i retningen av uskyldspresumsjonen.[27] Dommen nevner at lagringen er uavhengig av om den enkelte foretar en straffbar eller farlig handling. De registrerte blir utsatt for mulig etterforskning, uten å ha bidratt til dette.

Dersom data lagres om alle i tilfellet de skulle begå noe kriminelt, vil lagringen kunne komme i konflikt med uskyldspresumpsjonen i EMK art 6. I en avgjørelse fra 2008 kommenterer EMD at lagring av biometriske data av alle som har vært mistenkt i en sak undergraver uskyldspresumpsjonen fordi det ikke tar hensyn til hvorvidt den enkelte blir frikjent eller dømt for forbrytelsen.[28] Selv om lagringsplikten i denne saken var forskjellig fra datalagringsdirektivet, er det en viss likhet i grunnproblemet at uskyldige og skyldige behandles likt i en etterforskningssammenheng.

8 Klarhet og forutsigbarhet av loven

EMK art 8 annet ledd («*in accordance with the law*») stiller også krav til lovhjemmelens kvalitet. Hjemlene for inngrep i personvernet må være tilgjengelige, forutsigbare og formulert med tilstrekkelig presisjon slik at den enkelte kan justere sin atferd etter den.[29] Lover som hjemler ulike former for overvåkning er av EMD ansett for å gripe inn i en så sentral del av rettigheten at det stilles særskilte krav. Selv om det må skilles mellom trafikk- og lokasjonsdata, som er tema her, og telefonavlytting, der innholdet i kommunikasjonen kommer frem, kan det trekkes noen paralleller til EMDs praksis på området. I en avgjørelse fra 2008 krever EMD klare og detaljerte regler for telefonovervåkning inkludert varighet, lagring og sletting av data, bruk av og tilgang til data, prosedyrer for å sikre datakvalitet og konfidensialitet, samt tilstrekkelige sikkerhetstiltak for å hindre misbruk.[30]

27 Se dommens avsnitt 212.
28 S. and Marper v. the United Kingdom, (footnote17, ovenfor), § 122.
29 Se for eksempel Liberty and others v. The United Kingdom (app. 58246/00) 1. juli 2008, § 59 og Malone v. the United Kingdom (App. 8691/79) 2. august 1984, §§ 66-68.
30 Se S. and Marper v. the United Kingdom, (fotnote17, ovenfor), § 99.

Den rumenske forfatningsdomstolen fastslår at datalagringslovens bestemmelser ikke var tilstrekkelig tilgjengelige og forutsigbare. Etter domstolens syn åpner den for misbruk og ulik praktisering. Domstolen fokuserer særlig på lagring av andre relaterte data, i tillegg til trafikk- og lokasjonsdata. Den rumenske loven inneholdt som nevnt en plikt til å lagre ikke bare trafikk- og lokasjonsdata, men også tilknyttede data som er nødvendige for å identifisere den registrerte brukeren eller den registrerte kunden.[31] Det forble imidlertid uklart hva som teller som andre relevante data. I diskusjonen av kravet i EMK art 8 (2) om presise lover, trakk den rumenske dommen frem EMDs konklusjoner i Rotaru mot Romania[32] der kravet om forutsigbarhet ble tolket som et krav til tilstrekkelig presisjon i lovteksten. Det måtte være mulig for en vanlig person å forstå og innrette seg etter lovens krav. Videre viser domstolen til EMDs konklusjoner i Sunday Times mot Storbritannia,[33] der det ble stilt krav til at en vanlig borger skal kunne forutsi med tilstrekkelig grad av sikkerhet hvilke konsekvenser en bestemt handling kan medføre i henhold til loven.

Kravet til rettslig klarhet er også fremhevet flere steder i den tyske dommen. Dette gjelder særlig begrensninger av bruksformål for lagret data, herunder hva som i denne relasjonen er å regne for «alvorlig kriminalitet» samt krav til datasikkerhet (se nedenfor).

9 Krav til utlevering og bruk av data

Datalagringsdirektivet legger opp til at «[h]ver medlemsstat fastsætter i sin nationale lovgivning den procedure, der skal følges, og de betingelser, der skal være opfyldt for at få adgang til lagrede data» (art 4, annen setning). Den samme bestemmelse pålegger at prosedyren og betingelsene må være « i overensstemmelse med kravet om nødvendighed og proportionalitet».

I den tyske dommen ble proporsjonaliteten konkretisert på følgende måte: Jo mer inngripende lagringen er, desto strengere må kravene til databruken være. Domstolen krever derfor at lovgiver må regulere databruken på en presis måte, herunder i hvilke situasjoner lagret data kan innhentes, for hvilke formål de kan brukes og hvilket omfang databruken kan ha. Det betyr at ulike terskler må defineres for lovlig datainnhenting og bruk. Jo mer utstrakt databruken er, desto høyere bør terskelen være. Dommen krever at data omfattet av lagringsplikten kun kan brukes dersom det er nødvendig i sammenheng med etterforskning av mistanke om straffbare handlinger rettet mot *særdeles*

31 Datalagringslovens § 3.
32 Rotaru v Romania (App. 28341/95) 4. mai 2000
33 Sunday Times v Storbritannia (App. 6538/74) 26. april 1979

viktige samfunnsverdier (nedfelt i en katalog av straffebestemmelser) eller som forebygging mot farer for slike verdier. For øvrig krever domstolen at det lovreguleres hvordan myndighetene kan bruke utlevert data, herunder at bruken foretas omgående, at unødvendig data slettes, at alle data slettes når bruken ikke er lengre nødvendig, samt at slettingen dokumenteres. Dette krever blant annet at slike data blir identifisert særskilt i registrene. Omfanget av utlevert data må også være forholdsmessig. For eksempel måtte det skjelnes mellom utlevering av isolerte enkeltopplysninger, begrensete datasett og fullstendige bevegelses- og personlighetsprofiler.[34]

Lignende argumenter er også nevnt i den bulgarske saken: Loven åpnet for bruk av data i etterforskningen av en kriminalsak dersom det var behov for de av hensyn til den nasjonale sikkerhet. Domstolen kritiserte blant annet mangelen på henvisninger til andre relevante lover, herunder personvernloven.

Den tyske dommen fremhevet dessuten at beslutningen om utleveringen av data som hovedregel bør være forbeholdt en dommer. Denne må vurdere begrunnelsen for forespørselen om utlevering av data og må vurdere terskelen for inngrep, herunder om forespørselen er tilstrekkelig klar og om den velger ut relevante datasett. Videre krever dommen at det foreligger en mulighet for domstolskontroll i etterkant av databruken og et tilstrekkelig sanksjonsapparat knyttet til brudd på sikkerhetsplikten.

Den tyske dommen er meget vidtgående og nærmest dikterer en fullstendig omskriving av loven. Til sammenligning ønsket den rumenske forfatningsdomstolen eksplisitt å avstå fra å opptre som lovgiver og ga ingen føringer om hvordan en datalagringslov eventuelt kunne utformes for å være grunnlovsmessig. Det er mulig noen av de konkrete kravene i den tyske dommen også kan utledes av EMK art 8, basert på EMDs rettspraksis, for eksempel vedrørende telefonavlytting i Klass and others v Germany.[35] I vurderingen av om telefonavlytting var nødvendig i et demokratisk samfunn la EMD vekt på om det var tatt adekvate og effektive forholdsregler mot misbruk. Domstolen fant det uheldig at tillatelse til bruk av telefonavlytting ikke var underlagt rettens avgjørelse, og krevde lovregulering med spesifikke minimumskrav.

10 Transparens

En sentral likhet mellom den rumenske og den tyske dommen er at begge legger vekt på hvordan datalagringen og muligheten for bruk av lagret data vil

34 I denne sammenhengen spiller det en rolle om opplysningene blir filtrert for særlig beskyttelsesverdige telekommunikasjonsforbindelser. Se nærmere nedenfor, avsnitt 15.

35 Klass and others v Germany (App 5029/71) 6. september 1978.

kunne påvirke borgerne. Begge dommene peker således på et forhold som ofte preger personverndebatter: Virkningen av overvåkningen kan sammenlignes med et *panopticon*, der fangene blir sett av vaktene, mens fangene ikke kan se vaktene.[36] Slik mangel på transparens bidrar til følelsen av å være overvåket, uavhengig av om man virkelig blir utsatt for overvåkning. At lagringen og utleveringen skulle foretas uten borgernes umiddelbare kunnskap anses for å være spesielt problematisk i denne forbindelse. Dette er egnet til å generere en *«diffus bedrohliches Gefühl des Beobachtetseins»*,[37] noe som kan redusere befolkningens bruk av grunnrettigheter og friheter. En tilsvarende formulering finnes i den rumenske dommen, som mener at datalagringsplikten *«is sufficient to generate in the mind of the persons the legitimate suspicion regarding the respect of their privacy and the perpetration of abuses»*.[38] Domstolen viser til lignende argumentasjon fra EMD, hvor det trekkes frem at det bør unngås inngrep som innebærer *«destroying democracy on the ground of defending it»*.[39] Dette innebærer en begrensing av hvilke tiltak som kan iverksettes for å bekjempe alvorlig kriminalitet. Ikke ethvert tiltak som anses passende kan brukes i kampen mot terror, da det vil kunne undergrave sentrale rettigheter i et demokrati.

Særlig i den tyske dommen legges det derfor vekt på å oppnå en tilstrekkelig transparens om datalagringen og databruken ved å varsle den det gjelder. Riktignok forutsatte den tyske loven allerede slike varsler, men domstolen syntes at unntakene var for omfattende. Den krevde at unntak fra varsel kun bør være tillatt der dette kan hindre etterforskningen, og fastslo at en klar lovhjemmel for unntakstilfellene var nødvendig. Hemmelig databruk burde etter domstolens syn bare unntaksvis være tillatt. Dessuten krever dommen at det i disse tilfeller som hovedregel gis etterfølgende informasjon, samt at det i etterkant av databruken bør gis rett til å få avgjørelsen prøvet for en domstol.

Det er vanskelig å bedømme om en slik transparens vil være tilstrekkelig til å unngå følelsen av å bli overvåket, selv om den vil kunne ha en viss begrensende effekt. Problemet er at denne følelsen henger sammen med det vi ikke vet om overvåkningen, heller enn det vi vet. Det kan derfor antas at følelsen

36 Ideen om panopticon-fengselet ble opprinnelig utviklet av Bentham, og dens betydning for overvåkningsdebatten diskuteres, med henvisning til Foucalt, i L. A. Bygrave, (2002). Data protection law: approaching its rationale, logic and limits. Dortrecht, Kluwer, s. 109.

37 En «diffust truende følelse av å bli overvåket», se BVerfG, (ovenfor fotnote 14) avsnitt 212.

38 Romania Constitutional Court, decision no. 1258, 8. Oktober 2009. «Reţinerea acestor date în mod continuu, în privinţa oricărui utilizator de servicii de comunicaţii electronice (…)reprezintă o operaţiune suficientă să genereze în conştiinţa persoanelor bănuiala legitimă cu privire la respectarea intimităţii lor şi săvârşirea unor abuzuri.»

39 Klass and others v. Germany (App. 5029/71) 6. september 1978, § 49.

av å bli overvåket også vil være avhengig av hvilken tillit befolkningen har til myndighetene. Denne tilliten vil antagelig være noe forskjellig fra land til land, bl.a. ut i fra ulike historiske erfaringer med overvåkning. På den annen side vil konsekvent varsling om bruk av lagrede data på sikt antagelig kunne bidra til å bygge tillit.

11 Datasikkerhet

Mens den rumenske dommen ikke nevner datasikkerhet, stiller den tyske dommen meget strenge krav: For å være forfatningsmessig kreves særdeles høy datasikkerhet, fordi lagringen er meget inngripende (se over). Domstolen argumenterer med at data blir lagret hos private, som handler basert på økonomiske kriterier, noe som ikke nødvendigvis innebærer insentiver til høy datasikkerhet. Etter domstolens syn er det en høy risiko for ulovlig tilgang til data. Den tyske datalagringsloven inneholdt kun en ubestemt plikt til å sikre data, slik at utvalgte personer har tilgang til data. Utover dette var kravet til sikkerhet som ellers i telekommunikasjonssektoren.

Datasikkerhetseksperter har presentert ulike sikringsmetoder for domstolen, inkludert (i) en separat lagring av data på maskiner som ikke er tilknyttet nettet, (ii) asymmetrisk kryptering der nøkkelen oppbevares separat, (iii) et «fire øyers prinsipp», der datatilgang forutsetter to personer sammen og (iv) en protokollering av tilgang til data som kan kontrolleres i etterkant. Domstolen konstaterer at det ikke av den tyske forfatningen følger noen detaljerte krav til sikring. Likevel antyder den at alle ovennevnte datasikringstiltak (i-iv) i praksis vil være påkrevet.

Dessuten mener domstolen at det ikke er tilstrekkelig hvis krav til datasikkerhet åpner for en avveining der økonomiske faktorer skal tas hensyn til. På dette punktet er domstolen ikke tilstrekkelig presis. Den burde antagelig ha vist til en setning i loven, som sier at tekniske og andre sikkerhetstiltak er nødvendige, hvis den tekniske og økonomiske innsatsen som kreves står i forhold til betydningen av de rettigheter og innretninger som skal beskyttes.[40] Etter domstolens syn overlates konkretiseringen av sikkerhetsstandarden til tjenestetilbyderne, som må tenke økonomisk og som derfor ikke kan forventes å gjennomføre sikkerhetstiltak som anses å være for dyre.

40 § 109, andre avsnittledd, 7. setning TKG: «Technische Vorkehrungen und sonstige Schutzmaßnahmen sind angemessen, wenn der dafür erforderliche technische und wirtschaftliche Aufwand in einem angemessenen Verhältnis zur Bedeutung der zu schützenden Rechte und zur Bedeutung der zu schützenden Einrichtungen für die Allgemeinheit steht.»

Den tyske dommens vurdering av krav til datasikkerhet er særlig interessante. Domstolen krever et høyt sikkerhetsnivå, som ikke skal relativeres av økonomiske vurderinger. Når domstolen nærmest forbyr en kost/nytte vurdering, virker det nesten som om alle typer sikkerhetstiltak, bare de eksisterer i «state of the art», vil være påkrevet. Domstolen går her imot en trend innenfor regulering av risikospørsmål. Det antas vanligvis at nødvendigheten av sikringstiltak vil være kontekstavhengige, og bør bestemmes basert på en risikovurdering, som også innebærer visse økonomiske vurderinger. Men hvis det er forbudt å foreta en kost/nyttevurdering, vil ethvert teknisk tiltak som potensielt kan øke sikkerheten være påkrevet, uansett hvordan kostnadene står i forhold til nytten. Vi er enige i at dommens krav til datasikkerhet er hensiktsmessige for å begrense de negative effektene av datalagringen. Men når dommen fullstendig utelukker alle slags økonomiske vurderinger, virker det nærmest som om domstolen misforstår den økonomiske logikken i risikovurderingen. Konsekvensen kan være en plikt til å bruke uproporsjonalt dyre sikkerhetstiltak som har begrenset effekt.

12 Mindre strenge krav mht. IP-adresseopplysninger: begrenset anonymitet på nett

Den tyske dommen skiller klart mellom innhenting av opplysninger om brukere av IP adresser[41] (heretter IP brukeropplysninger) og andre data. Domstolen mener at vilkårene for innhenting av opplysninger om bruker av en kjent IP adresse kan være lavere: Dommen tillater at IP brukeropplysninger kan utleveres for å tjene etterforskning av *enhver* type kriminalitet, inkludert de fleste typer av mindre bøtestraffer («Ordnungswidrigkeiten») og all fareforebygging. Kravene er altså mindre strenge enn ellers.[42]

Dette skillet er av prinsipiell betydning, og dersom domstolen har rett i sin argumentasjon bør vurderingen ha overføringsverdi. Domstolens vurdering er begrunnet i at innhenting av IP brukeropplysninger er mindre krenkende for personvernet enn andre trafikk- og lokasjonsdata, bl.a fordi dette er en punktvis opplysning, som ikke kan brukes til å generere personprofiler. Dommen fokuserer særlig på situasjon der myndigheten allerede har en (dynamisk) IP adresse, men mangler kunnskap om brukeren av denne på et bestemt tidspunkt. IP adressens form ligner på et telefonnummer, men funksjonen er annerledes, da IP brukeropplysninger også sier noe om innholdet i kommunikasjonen, for

41 En IP-adresse er et nummer som identifiserer en enhet (for eksempel en datamaskin) i et nettverk som benytter Internet Protocol (IP).

42 Om kravene for utlevering og bruk av annen data se ovenfor, avsnitt 9.

eksempel websiden som besøkes. Når man åpner for innhenting av IP brukeropplysninger uten like strenge krav som for andre datatyper, innskrenker dette brukerens anonymitet på Internett. Etter domstolens syn er dette akseptabelt, «fordi Internett i en rettsstat ikke kan være et rettstomt rom».[43] Forventningen om anonymitet må vurderes opp mot andre hensyn, særlig betydningen og verdien av IP brukeropplysninger for etterforskning av IT-relatert kriminalitet. Forventningen om anonymitet på Internett må altså vike for etterforskningshensyn uten at det kreves en konkret mistanke om alvorlig kriminalitet.

13 Forbud mot direkte tilgang til data

Myndighetenes tilgang til data kunne organiseres slikt at de henter ut data (ved direkte oppslag) fra tilbyderne. Selv om den tyske lovgivningen ikke hadde lagt opp til direkte tilgang, la domstolen vekt på at myndighetene ikke kunne ha slik tilgang. Dette følger, ifølge dommen, blant annet av at datainnhenting som hovedregel krever en forutgående domsavgjørelse. I Bulgaria synes myndighetene derimot å ha hatt en nokså direkte tilgang til data, men vi kjenner ikke detaljene om dette. Ifølge omtaler på Internett ga den bulgarske bestemmelsen myndighetene tilgang til server med alle data som var lagret av Internett- og teletilbydere. Tilgangen var ikke underlagt rettens avgjørelse. Fem av rettens medlemmer gikk inn for å annullere bestemmelsen under henvisning til at den ikke satte grenser for tilgangen til serveren og ikke omfattet mekanismer med henblikk på beskyttelse av retten til privatliv, som er vernet i Bulgarias konstitusjon.

De ulike modellene for innsamling og tilgang til data har en vesentlig betydning for hvordan data kan brukes i etterforskningssammenheng. Slik den tyske lovgivningen var lagt opp forhindret den desentrale lagringen *data mining,* dvs. søking etter mønstre i data. I motsetning til sine bulgarske kollegaer hadde tyske myndigheter ikke denne muligheten.

14 Etterretningens bruk av lagret data

Lagret telekommunikasjonsdata er ikke bare av interesse for politiet, men også for etterretningen.

Den tyske dommen stiller meget strenge krav til etterretningens databruk. Dette gjøres ved å likestille kravene til bruk av data ved etterretningstjenesten og politiet. I generelt etterretningsarbeid foreligger det sjelden en konkret mistanke. Likestillingen av etterretningstjenesten innebærer derfor i praksis at de

43 Se dommens avsnitt 260.

lagrede data blir umulig å bruke til etterretningsformål. Domstolen sier rett ut at dette resultatet er direkte ønsket.[44]

Den rumenske domstolen synes ikke å gå like langt, siden den ikke diskuterer hvorvidt etterretningstjenestens tilgang til data er grunnlovsstridig. Men domstolen kritiserer ordlyden i datalagringslovens § 20, som henviste til «trusler mot Romanias grunnleggende sikkerhetsinteresser» uten å nærmere definere disse. Bestemmelsens ble ansett å åpne for at også andre organer, i tillegg til etterforsknings- og etterretningsorganer kunne gis tilgang til de lagrede data, uten at disse organene hadde en rolle som omfattet bekjempelse av alvorlig kriminalitet[45].

15 Vern av anonymitet i tillitsrelasjoner

Den tyske datalagringsloven ble også ansett å være uforholdsmessig fordi den ikke ga noen beskyttelse av anonymitet i bestemte tillitsrelasjoner, som for eksempel ved anonym telefonrådgivning. Etter domstolens syn er en slik beskyttelse påkrevet, i hvert fall for særlig beskyttelsesverdige tillitsrelasjoner. Utlevering av slike trafikkdata strider mot proporsjonalitetsprinsippet, så de må ifølge dommen filtreres ut før data utleveres til myndighetene.

Lignende argumenter kan antagelig brukes i forhold til pressens kildevern, samt fortrolighet mellom advokat og klient, noe som har vært fremme i den norske debatten. Det kan ikke utelukkes at en slik filtrering vil kunne begrense nytten av data for politiet, særlig dersom slike tillitsrelasjoner misbrukes for å hindre en mulig etterforskning. Filtrering av data for tillitsrelasjoner er et element som ikke virker tilstrekkelig vurdert i det norske høringsnotatet.[46] Trolig kan det spille en rolle for vurderingen at det er uklart hvordan en slik løsning ville kunne se ut i praksis.[47]

---

44 Se dommens avsnitt 234.

45 « utilizarea sintagmei «pot avea» induce ideea că datele la care se referă Legea nr.298/2008 nu sunt reținute în scopul exclusiv al utilizării acestora numai de către organele statului cu atribuții specifice în protejarea securității naționale și a ordinii publice, ci și de alte persoane sau entități, din moment ce acestea «pot», și nu «au», acces la aceste date, în condițiile legii»

46 Høringsnotat utsendt fra Samferdselsdepartementet, Justis- og politidepartementet og Fornyings-, administrasjons- og kirkedepartementet 08.01.2010, se http://www.regjeringen.no/nb/dep/sd/dok/hoeringer/hoeringsdok/2010/horing---datalagring.html?id=590001.

47 Man måtte nærmest tenke seg en offentlig forvaltet liste over identifikatorer (telefonnumre, IP adresser og e-post adresser) som brukes av bestemte privilegerte aktører til bestemte beskyttelsesverdige formål.

15 Avsluttende bemerkninger

Avslutningsvis vil vi kort sammenfatte de viktigste argumentene som har kommet frem i dommene.

Fordi proporsjonalitetsprinsippet er sentralt i forhold til EMK, gir dommene visse retningslinjer for hvordan en datalagringslov kan være forenlig med konvensjonen, og derved hvilke hensyn som bør tas ved en eventuell norsk lov om datalagring. Mens alle tre dommene tar utgangspunkt i dette prinsippet, er de konkrete vurderingene noe forskjellige. Den vesentligste forskjellen er at man i Romania anser selve lagringsplikten som uproporsjonalt, mens den tyske domstolen i stedet bruker proporsjonalitetsprinsippet til å utlede strenge krav til datalagringsloven. Uansett vil strenge krav til datalagringen gjøre datalagringen mer proporsjonal, fordi dens negative konsekvenser blir mer begrensede. De personvernmessige betenkelighetene ved datalagring kan til en viss grad tenkes avhjulpet av strenge krav til datasikkerhet. I tillegg er det behov for strenge regler for utlevering og bruk av data, samt en effektiv domstolskontroll. Videre bør reglene legge til rette for en transparent databruk, for å motvirke følelsen av å være overvåket.

PRIVACY REGULATIONS ON BIOMETRICS IN AUSTRALIA[1]

Yue Liu

Abstract

This paper aims to provide an analysis of the current regulatory environment, at the federal level, of privacy protection concerning biometrics in Australia. The study only focuses on the federal Privacy Act 1988 (Cth) and the Biometrics Institute Privacy Code. The discussion is based on the legal concerns of the use of biometrics, and an analysis is made concerning the implications of privacy protection sources.

Key words

Privacy regulations, biometrics, personal information, Australia

1 Introduction

Concerns about biometrics are of particular importance in light of the Australian government's adoption of the e-passport[2] to be in compliance with the U.S. requirement for visa-waiver countries, as well as by Australian customs authorities to expand the SmartGate scheme,[3] along with the rollout of

1 Originally published in Computer Law & Security Review Volume 26, Issue 4, July 2010, Pages 355-367

2 The next generation of Australian passport—the 'ePassport'—was introduced on 24 October 2005. For further research see the Department of Foreign Affairs and Trade (2009). «The Australian ePassport.» Retrieved 15.02.2010, from http://www.dfat.gov.au/dept/passports/.

3 It has been reported that the self-service facilities are installed at Sydney, Adelaide, Brisbane, Cairns, Melbourne and Perth international airports. SmartGate is an automated border processing system. It is a secure and simple system that performs the customs and immigration checks normally made by a customs officer when a person first arrives in Australia. It uses the data in the ePassport and face recognition technology to perform the customs and immigration checks that are usually conducted by a Customs and Border Protection officer.

SmartGate can be used by Australian and New Zealand ePassport holders, aged 18 or over. It will be gradually opened to other nationalities that have ePassports. For more information on the Australian ePassport please go to: http://www.passports.gov.au/ , Last visited Jan 11, 2010

biometric databases by immigration authorities in connection with processing visa applications.[4] The growing importance of identity management and the spreading use of biometric technology have precipitated vigorous debate in Australia about the legal regulation of personal information and reasonable limits of privacy. Some of that debate focuses on plans to roll out extensive facial recognition systems at Australian airports[5] and the introduction of biometric information in smart cards[6]. Discussion from a legal perspective is manifest largely in a paper by the previous federal privacy commissioner, Mr. Crompton, in documentation regarding the drafting of the *Privacy Code* of the Biometrics Institute,[7] and, more recently, in the Australian Law Reform Commission's report, *For Your Information*, in which biometric issues are tackled fairly extensively. Otherwise discussion on biometrics from a legal perspective is quite limited.

This paper aims to provide an analysis of the current regulatory environment, at the federal level, of privacy protection concerning biometrics in Australia. As Australia is a federation, the study only focuses on the federal Privacy Act 1988 (Cth) and the Biometrics Institute Privacy Code. These two instruments provide the central privacy and data protection rules for regulation of biometrics in the private sector and the federal government sector. There are a small number of state laws on privacy and data protection but these are not analysed as they are of relatively minor significance for the biometrics-related concerns here.

Section 2 of this paper briefly describes the relevant sources of privacy rights in Australia, with special focus on the Privacy Act 1988 and the Biometrics Institute Privacy Code. Section 3 details the legal concerns of the

4 The Department of Immigration and Citizenship is reportedly building a database of facial, fingerprint, and iris scans that will be linked to a global processing system and intelligence and security databases. The biometric data of New Zealanders and other foreign nationals entering Australia could be permanently stored in a central repository for identity verification and cross-checking between federal government departments, national and international anti-identity fraud bodies, and border control systems. This information will be stored in the department's central Identity Services Repository .See, Aussies to stockpile Kiwi biometrics in central database, at http://computerworld.co.nz/news.nsf/news/4C244AE1ED29925CCC25731E000055D0 , last accessed,12.Jan, 2010

5 Clark, R. (2003) «Smart Gate: a face recognition trial at Sydney airport.» Retrieved 15.02.2010, from http://www.rogerclarke.com/DV/SmartGate.html.

6 Australian Privacy Foundation (2004). «Submission to Senate Legal & Constitutional Committee Inquiry into the Privacy Act 1988, Annex D, Biometrics Institute Draft Privacy Code of Practice.» Retrieved 15.02.2010, from http://www.aph.gov.au/senate/committee/legcon_ctte/privacy/submissions/sub32ann_d.pdf.

7 The Biometrics Institute Privacy Code was approved by Australian Privacy Commissioner Karen Curtis 19.07.2006, and it came into operation 01.09.2006.

use of biometrics, and an analysis is then made concerning the implications of privacy protection sources. The paper concludes in Section 4 with suggestions for potential legislation necessary to protect privacy in the biometric context.

2 Sources of privacy protection

Australia is a federation of former British colonies. The federal (Commonwealth) Parliament has specific legislative powers according to Section 51 of the Constitution. In Australia there has until recently been no recognition of a general tort of breach of privacy.[8] Actions for breach of confidence, defamation, trespass, or nuisance are occasionally used in support of privacy rights (Privacy International 2004). The International Covenant on Civil and Political Rights (ICCPR) Article 17 can also provide privacy protection to Australians.[9] Australian privacy laws are contained in a variety of Commonwealth, State, and Territory Acts. The Commonwealth legislation, according to Section 109 of the Constitution, prevails over State or Territory privacy legislation to the extent that these laws are inconsistent. At the federal level the Privacy Act 1988 (Cth) is the main source of protection that is relevant to biometrics.[10]In addition, the industry self-regulated Biometrics Institute Privacy Code also has special value as it is one of the few existing biometric-specific privacy codes.

2.1 The Privacy Act

The Federal Privacy Act incorporates the amendments made to it by the Privacy Amendment (Private Sector) Act 2000 (Cth). Before this amendment the Act mainly covered only Commonwealth and ACT government agencies, but the scope is now wider and encompasses some private sector actors. The Act covers the collection, use, and disclosure, as well as the quality and securi-

8 See *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd* (2001) 185 ALR 1. See also Butler (2005)

9 E.g., in *Toonen v Australia* (1994) 1 PLPR 50, the UN Human Rights Committee found that Australia was in breach of the provision in the ICCPR because of legislation in an Australian state (Tasmania) which criminalised homosexual conduct in private. The Australian Commonwealth Government then legislated to nullify the effect of the Tasmanian legislation. No cases involving Australia have been brought before the Human Rights Committee with respect to data protection issues, let alone biometrics.

10 There are also some other laws and regulations that are relevant to privacy and data protection, such as The Spam Act 2003 (Cth), Medical care and Pharmaceutical Benefits Programs Privacy Guidelines, Data-Matching Program (Assistance and Tax) Act 1990 (Cth), National Health Act 1953 (Cth), and Telecommunications Act 1997 (Cth). These are, though, of relatively marginal significance for biometrics-related concerns addressed in this paper.

ty of personal information. It provides various basic privacy principles depending on what area it is regulating. There are 11 Information Privacy Principles (IPPs) governing the handling of personal information by Commonwealth and ACT government agencies as set out in Section 14.[11] They specify matters such as: 1) the purpose and manner of collecting personal information (IPPs 1–3); 2) the way the personal information should be stored (IPP 4); 3) the way the records are to be kept (IPPs 5, 8); 4) access to and revision of the personal information in records (IPPs 6–7); 5) the reuse of the personal information kept in records (IPPs 9–10); 6) limitations on the disclosure of the personal information (IPP 11).

In addition, the Act applies to the handling of personal information by health service providers and private sector organisations that earn more than $A3 million annually. It establishes minimum privacy standards for the Australian private sector called National Privacy Principles (NPPs).[12] Organizations are required to comply with the NPPs unless they are exempt. The Principles are ten in number and deal with 1) collection and use of personal information (NPPs 1–2); 2) the quality and security of personal data stored (NPPs 3–4); 3) the level of openness, access, and revision of personal information by data subjects (NPPs 5–6); 4) the adoption of identifiers (NPP 7); 5) anonymity (NPP 8); 6) trans-border data flows (NPP 9); and 7) sensitive information (NPP 10). The legislation does not generally apply to small businesses (i.e., businesses with an annual turnover of less than $A3 million) and it does not apply to political parties, employee records held by current or former employers of the employees, or to acts and practices of the media in the course of journalism.[13]

The two sets of privacy principles share many similarities but are, in places, inconsistent and unclear. A unified privacy protection system has recently been proposed by the Australian Law Reform Commission (ALRC) in order to resolve much of the complexity in the current provisions[14]. At the time of writing, it is not clear exactly how the ALRC proposals will be implemented.

---

11 See Office of the Federal Privacy Commissioner (2001 b). «Plain English Guidelines to Information Privacy Principles.» Retrieved 16.02.2010, from www.privacy.gov.au/publications/page1.html#1

12 Office of the Federal Privacy Commissioner (2001 a). «Guidelines to the National Privacy Principles, September 2001 «. Retrieved 16.02.2010, from http://www.privacy.gov.au/materials/types/guidelines/view/6482#c1.

13 For more information on exemptions and coverage go to information sheet 1-2001 Overview of the Private Sector Provisions, at <http://www.privacy.gov.au/publications/IS12_01.html>, accessed 11.01.2010.

14 Australian Law Reform Commission (2008 a). «ALRC report 108: For your information: Australian Privacy Law and practice.» Retrieved 15.02.2010, from http://www.austlii.edu.au/au/other/alrc/publications/reports/108/

2.2 Biometrics Institute Privacy Code

The independent Biometrics Institute representing the Australasian biometrics industry and users received approval from the federal Privacy Commissioner on 19 July 2006 for a binding Privacy Code. The Code is an industry self-regulatory code. It came into operation on 1 September 2006 and is intended to be ratified by the organizations in the biometrics industry in Australia on a voluntary basis. Once the Code is ratified by a certain organization, it will be bound by the Code instead of the NPPs.

This regime is based on the provisions of the Privacy Act 1988 which give the option for organizations to develop their own privacy codes which, when approved by the federal Privacy Commissioner, replace compliance with the NPPs. Section 18BA provides that «an organisation may apply in writing to the Commissioner for approval of a privacy code».[15] The Privacy Commissioner must approve each such code in accordance with the Act. Where an organization consents to be bound by an approved code, the code operates in place of the NPPs until the organization ceases to be bound by the Code.

The Biometrics Institute Privacy Code largely replicates the wording of each of the NPPs (from NPP1 to NPP10) but incorporates higher standards of privacy protection in relation to certain acts and practices concerning employee records that otherwise would be exempted from coverage by the Privacy Act. It seeks, inter alia, to give guidance on how privacy principles shall be applied to the collection and use of biometrics. At the same time, the Code includes three new supplementary Privacy Principles (11–13) specifically concerning biometric technology.

Principle 11 prescribes an array of security measures (including encryption) for protecting biometric information either while in storage or transmission. It supplements the data security obligations in NPP 4.

Principle 12 prescribes a set of measures that are aimed at enhancing data subjects' control over biometric information collected on them. The measures involve requirements of notice, consent and withdrawal of consent. Particularly significant is a prohibition on «secondary analysis or function creep of biometric information» without the data subjects' «express free and informed consent». The measures supplement NPPs 1.3, 1.5, 2 and 4.

15 «Organisation» is defined in s. 6C as any entity that is not a small business operator, a registered political party, an agency, a State or Territory authority, or a prescribed instrumentality of a State or Territory. A «small business operator» is defined in s. 6D as a business that has an annual turnover of $3 million or less and, subject to some exceptions, is exempt from the legislation. A business may be exempt from the Privacy Act because it does not come within the definition in s. 6C; it may also choose to be treated as an organisation (see s. 6EA). The Biometrics Institute has chosen to be treated as if it were an organisation.

Principle 13 deals with accountability matters. It requires, inter alia, disclosure of the purposes of biometric systems, third party auditing of such systems, together with holistic privacy management (including the use of privacy impact assessments) of such systems. These requirements augment NPPs 1, 4 and 5.1.

3 Coverage of Privacy Act and Privacy Code

3.1 Definition of Biometrics

According to the Biometrics Institute Privacy Code,[16] biometrics refers to «automated methods for identifying and/or verifying an individual on the basis of some biological or behavioural unique characteristic of the individual» (Section E). Concomitantly, a «biometric» is «a biological or behavioural unique characteristic of an individual which is captured for the purpose of identification and/or verification of the individual» (Section E). As for «biometric information», this is defined as follows:

> *Biometric information is any data that can be used to biometrically identify an individual. This data includes, but is not limited to, images, sounds, chemical or geometric properties. It also includes any information encrypted or unencrypted that is derived from these raw acquired biometrics, such as biometric templates or filtered or pre-processed data … (Section E).*

If we consider the definitions of «biometrics» and «biometric» first, they emphasise the «unique» characteristic of an individual. This is somewhat surprising as not all biometrics are unique. Furthermore, verification usage is mentioned as one purpose in parallel with identification, yet the definition of biometric information omits reference to verification or authentication.

The definition of biometric information is nonetheless to be lauded for its relative degree of clarity. A clear definition of biometric information or biometric data has not been found in any legal documents in Europe concerning privacy and biometrics, but it is generally indicated there that biometric information shall include both the raw biometric image and the biometric template.[17] By contrast, the Biometric Identifier Privacy Act enacted by the State

16 Hereinafter also referred to simply as the «Privacy Code».

17 See The Consultative Committee of Convention 108 (2005) «the biometric data, either the picture or the template….».

of New Jersey in the USA provides only an unclear and imprecise definition of what can be considered a biometric identifier: «retina or iris scan, fingerprint, voiceprint or record of a hand or face geometry.» It fails to give an accurate description of the main characteristics of biometric information in general, and only provides a list of examples instead. That list seems to be exhaustive, but it actually excludes many other aspects of biometric information in the general sense, and it remains nebulous as to whether it refers to the raw biometric image or the biometric template. Compared with both the European understanding of biometric data and the definition contained in the New Jersey legislation, the Privacy Code's definition includes more than raw biometric images and biometric templates, as it states «…such as biometric templates or filtered or pre-processed data,» which tends to include more relevant data that may appear during the biometric processing.

Although the attempt to give a legal definition of biometric information in the Privacy Code can be seen as a leap forward compared with the mentioned definitions, the current definition of *biometrics* and *biometric information* in this code needs to be delineated more clearly and precisely. The code defines biometric information «as any data that *can be* used to biometrically *identify* an individual» (emphasis added). First of all, the word «biometrically» is obscure, although the meaning might be deduced from the definition of «biometrics» (i.e., «automated methods for identifying and/or verifying an individual on the basis of some biological or behavioural unique characteristic of the individual»). Also, instead of using the typical wording «for the purpose of identification and verification,» the specific use of the words «can be» is important. Does this indicate that the Code accepts that biometric information is generally «identifiable,» since by its nature it is created to identify people? Or does it mean to exclude some part of biometric information that is not identifiable—if there is any?[18] Since biometric information can be used for authentication as well as for identification purposes, does this specification of the words «can be» indicate that no matter what purposes the biometrics are intended to be used for, biometric data in general are able to identify people?

3.2 Personal information and identifier

The Privacy Act (Cth) section 6 defines personal information to be:

18 There are a number of controversial discussions on whether biometric data can be made to be not identifiable. Cf. Liu (2008). Identifying Legal Concerns in the Biometric Context, *Journal of International Commercial Law and Technology,* Vol3 (4) 45-54

> *Information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion.*

This definition is replicated in the Biometrics Institute Privacy Code section E. At the same time, the Code operates also with the concept of «biometric information», which is defined such that it appears to be a category of «personal information». This approach conforms with an earlier analysis by Crompton of when biometric information may be personal information[19]. Crompton concluded that the Privacy Act will apply to biometric information when it is clearly information about 'an individual,' and when biometric information is created to identify people[20]. Biometric data, by their nature, are intimately and specifically linked to a certain person. Even if sometimes collected only for authentication, there is the possibility that these data *can be* (as stated in both the Privacy Act and the Privacy Code) related to an identifiable individual. In this respect biometric information falls within the scope of «personal information», and so the Privacy Act should be applicable.

The Privacy Act also contains a principle dealing explicitly with identifiers; NPP 7 defines an identifier as including «a number assigned by an organization to an individual to identify uniquely the individual for the purposes of the organization's operations.» However, an individual's name or ABN (as defined in A New Tax System (Australian Business Number) Act 1999 (Cth)) is explicitly excluded as an identifier. A similar provision does not appear in the IPPs, which indicates that it only applies to private sector actors.

Biometric information as code that relates to physical or behavioural characteristics of individuals might be included in the current definition of an identifier. According to the Revised Explanatory Memorandum to the Privacy Amendment (Private Sector) Bill 2000, the identifiers are «not limited to letters and numbers,» although an identifier «will often contain either, or both.»[21] However, NPP 7 also requires that the identifier «identify uniquely the individual for the purpose of the organization's operations.» While biometric information is relatively unique to an individual, a number of factors may affect the accuracy of a match and the quality of a certain biometric template, which as a result may affect the «uniqueness» of the biometric identifier. As a result, it has

19 Crompton, M. (2002). «Biometrics and Privacy.» *Privacy Law and Policy Reporter.* Vol. 9(3): 53-58.

20 Ibid.

21 Revised Explanatory Memorandum, *Privacy Amendment (Private Sector) Bill 2000* (Cth), para361

been suggested that an amendment to the definition may be required to ensure that biometric information is in fact captured by the «identifier» principle[22].

3.3 Exemptions

The Privacy Act exempts certain specified actions, practices and organizations from its coverage. Section 7B exempts individuals in a non-business capacity, organisations acting under commonwealth contract, employee records, journalism, and organisations acting under state contract, and s. 7C exempts political acts and practices. Of these various exemptions, those for employee records and small businesses may appear to be most critical where biometrics is concerned. If these two exemptions continue to pertain, a significant number of biometric applications would be able to escape from the data privacy legislation in Australia, which would render all the principles and considerations therein meaningless for those applications. However, the Biometrics Institute Privacy Code includes employee records, which is an improvement on the Privacy Act. Unfortunately, however, the Code still keeps the small business exemption, even though that exemption is actually more problematic than that for employee records – as discussed below.

Using biometric technology as an authentication method for computer network access and access to office buildings is becoming more and more common. For example, as already noted, in the Australian Woolworths supermarkets, finger-imaging technology is used to monitor time and attendance for about 100,000 employees. If these records are regarded as employee records, it will mean none of the employees' biometric data will be protected by the Privacy Act. The vacuum created by the exemption is supposed to be filled by state government legislative initiatives on workplace privacy, but the legislation so far enacted would seem to be far from adequate, at least in the context of biometrics. For instance, the main legislation on workplace privacy in Victoria is the Surveillance Devices Act 1999, which covers certain uses of devices for «data surveillance», «optical surveillance» or «tracking». Arguably, biometric equipment might be regarded as a «tracking device» under the Act. Such a device is defined as «an electronic device the primary purpose of which is to determine the geographical location of a person or an object» (s. 3(1)). But if the biometric equipment's primary purpose is to authenticate or identify people, it would seem difficult to argue that such equipment is covered by this definition. As for other states, most of them (with the exception of New South Wales) have yet to enact workplace privacy legislation, which means that in

22 Supra note 13 p.1035

most if not all Australian jurisdictions, the use of biometric data as employee records is left inadequately regulated.

It is even more difficult to find a justification for the small business exemption in the Privacy Act. Small businesses comprised up to 94% of Australian business in 2000,[23] which indicates that many consumers in Australia may enjoy comparatively weak protection of their privacy interests when interacting with small businesses. It can be reasonably assumed that a significant (and increasing) portion of these enterprises are adopting biometric technology as authentication or identification methods for various commercial purposes. The deficiency of the small business exemption is not only restricted to the biometric scenarios; rather, it is a deficiency of the Privacy Act in general. A number of criticisms of the exemption have been expressed. Considering the relevance to the protection of privacy in biometrics, they can be summarised as follows:

1. Privacy rights do not disappear just because a consumer happens to be dealing with a small company.[24]
2. The $3 million annual turnover threshold for the exemption is not usually apparent to the consumers.[25]
3. By the expedient splitting of any constituent businesses into sub-businesses before they reach the $3 million threshold (s. 6D(4)(a)), big businesses can escape completely from the operation of the Act.[26]

3.4 Sensitive information

Biometric information does not fit neatly into the category of «sensitive information,» besides its health and genetic-related nature. However, biometric information may carry greater risks than other forms of information due to its linking and tracking ability, its relative uniqueness and permanence, and its intimate link to physical characteristics. For these reasons, it is pertinent to discuss whether and how biometric information can be categorised as «sensitive information» under the Privacy Act 1988 (Cth).

---

23 Australia Department of Employment (2000). «Workplace Relations and Small Business to the Standing Committee on Legal and Constitutional Affairs' inquiry into the provisions of the 2000 Bill.» Retrieved 15.02.2010, from http://www.aph.gov.au/HOUSE/committee/laca/Privacybill/submiss.htm.

24 Supra note 23 p.34

25 Privacy Commissioner New South Wales (2005). «Privacy New South Wales Submission to the House of Representatives Standing Committee on Legal and Constitutional Affairs on the Privacy Amendment (Private Sector) Bill 2000.» Retrieved 16.02.2010, from http://www.aph.gov.au/HOUSE/committee/laca/Privacybill/sub62.pdf.p.7

26 Ibid. P.34

The concept of «sensitive information» is defined in s. 6(1) of the Privacy Act. Sensitive information is a subset of personal information. It includes

> *(a) information or an opinion about an individual's (i) racial or ethnic origin; or (ii) political opinions; or (iii) membership of a political association; or (iv) religious beliefs or affiliations; or (v) philosophical beliefs; or (vi) membership of a professional or trade association; or (vii) membership of a trade union; or (viii) sexual preferences or practices; or (ix) criminal records that also contain personal information; or (b) health information about an individual; or (c) genetic information about an individual that is not otherwise health information.*

This definition is broader than the definition of «special categories of personal information» in the EU Data Protection Directive, in that it clearly specifies that genetic information is sensitive information. By contrast, the Directive does not explicitly mention genetic information, though the latter is usually regarded as relevant to health information in most cases.

The NPPs provide additional restrictions on the collection of sensitive information; it is subject to a higher level of privacy protection than other «personal information» handled by organisations (NPP 10). However, the IPPs which apply to government agencies contain no equivalent restrictions, which is problematic. The Biometrics Institute Privacy Code includes an additional principle (Principle 12.3) similar to the scope of protection provided for sensitive information by NPP2.1(a):[27]

> *Secondary analysis or function creep of biometric information collected for purposes such as authentication or identification is not permitted without express free and informed consent. For example, biometric information collected for the purposes of authentication and identification shall not be used to examine that information in search of genetic patterns or disease identification without express free and informed consent.*

27 NPP 2.1(a) states: «An organization must not use or disclose personal information about an individual for a purpose (meaning the secondary purpose) other than the primary purpose of collection unless: (a) both of the following apply:
(i) The secondary purpose is related to the primary purpose of collection and, if the personal information is sensitive information, directly related to the primary purpose of collection;
(ii) the individual would reasonably expect the organization to use or disclose the information for the secondary purpose.»

This may indicate that biometric information is classified as sensitive information in this Code, and thus is provided with a higher level of protection.

The ALRC has proposed that biometric information should be given the same level of protection as other information that is currently treated as sensitive information; concomitantly, the definition of sensitive information should be amended to include biometric information[28]. The ALRC intends to limit the type of biometric information to be included in the definition of sensitive information. It proposes that the sensitive information should only include «biometric information collected for use in automated biometric authentication and identification systems and biometric template information»[29]. This opinion is in accordance with the view of the Office of the Privacy Commissioner (OPC), which states, «It may be impractical and undesirable for all biometric samples to be included under the definition of sensitive information, especially where there is no intention to use the sample for biometric matching or identification.»[30]An example is given that taking a photograph of a person shall be excluded. This opinion is reasonable to the extent that it takes into account the practicability of enforcement. But it may also create a loophole for easily circumventing the protection of biometric information as sensitive information. Because «intention» is a subjective term, suppose in practice, biometric information may be collected from an individual without consent since it is classified as ordinary «personal information» by a private agency, as there is no *intention* to use it for identification and authentication, and thus no biometric template is created. «Intention» could change from time to time, once the collection is made; therefore, it becomes difficult to control the biometric information at the level of its individual source. All that can be done is to trust the collector.

4 Information Privacy Challenges of Biometrics

4.1 Unauthorised collections: Notice and consent

To realise the maximum control by a data subject over personal information, their free and informed *consent* is indispensable. However, as a basic means of «controlling» personal information during the primary collection, consent

28 Supra note 13 p.451
29 Ibid.p.452
30 Australian Law Reform Commission (2008b) ALRC Submission, retrieved 02.02.2010 from www.austlii.edu.au/au/other/alrc/publications/dp/72/3.rtf p. 212

is not clearly required by the Privacy Act 1988 (Cth). With respect to the federal government sector, IPP 1(1) requires that the collection of personal information be for lawful *purposes* and by lawful *means*. Inconsistently, NPP 1, for the private sector only, requires that the *means* of collection be lawful. In addition, IPP 2 requires that, where *practicable,* the individual concerned is to be made generally aware of the purpose and to whom the information will be disclosed. Solicitation is required for the collection of private information from the individual concerned, though it does not mention that *consent* is required under any circumstances. In NPP 1.3 the requirement of «practicable» is replaced using the wording «must take reasonable steps to ensure.»[31] The Biometrics Institute Privacy Code generally applies the same wording as in NPP 1, but its supplementary Principle 12.1 emphasises that «enrolments in biometric systems shall be voluntary, unless required by law». This indicates that the Privacy Code prohibits compulsory collection of biometric information in the private sector, unless the law regulates otherwise. However, it is not clear when it should be regarded as «required by law». If «law» includes the Privacy Act, this would be very problematic as it would undermine the consent requirements of the Code. As noted above, the Act does not require consent for primary collection. Thus, the collection of biometric data can be compulsory under the Privacy Act. Individuals have no choice or control whatsoever concerning collection, use, and disclosure of their personal information for the primary purpose of collection.

However, both the NPPs and IPPs forbid the covert collection of biometric data, as they both require that information be collected by lawful and fair means (IPP 1, NPP 1.2). The notice requirements form an important foundation for prohibiting covert collection. In the Guidelines to the National Privacy Principles and in the Plain English Guidelines to the Information Privacy Principles, the Office of the Federal Privacy Commissioner has interpreted this to mean that information must not be collected covertly, although exceptions have been made for investigations of criminal offences[32]. However, even if notice is given when collecting biometric information, it is not guaranteed in practice that the notice clearly includes all of the required information or provides links to such information[33]. In the context of biometrics, the «notice» becomes even more problematic. The understanding of biometric technology

31 The nebulous words «practical» and «reasonable steps» are interpreted by balancing a number of possible factors. See Supra note 11

32 Supra note 10 and 11

33 Australian Privacy Foundation (2005). «Submission to Senate Legal & Constitutional Committee Inquiry into the Privacy Act 1988.» Retrieved 15.02.2010, from http://www.privacy.org.au/Papers/SenateCteePrivacyAct0503.rtf p.16

is quite limited if not nonexistent among lay persons; moreover, most people are not aware of the privacy and security risks they are exposed to by providing their biometric data. Science fiction movies and misleading advertisements appear to be the most widespread ways of getting to know about the technology. Therefore, how and to what extent the amount of information should be presented to the data subjects become crucial. Notice consisting of a short and concise statement with links to further resources would be useful and desirable.

NPP2.1 and IPP11 (b) both require consent for secondary collection whenever *practicable*. However, this principle can be greatly abused. As mentioned above, lacking a clear and concise notice, many individuals are likely to be irritated by the length of tedious statements, and might tend to simply choose to sign the consent without being clearly informed. In addition, it is likely that few individuals will challenge the request due to the imbalance of power between individuals and organizations. When they have no better alternatives, they might simply give their consent because of the convenience of doing so. This might pose an even more serious problem in using the biometric technology. An obvious advantage of biometric technology is that it offers convenience in contrast to the old authentication or identification methods, and it is arguable that people generally do not understand the danger of secondary disclosure of their biometric information. How to ensure the *free and fully informed choice* to the individual concerned about biometrics is another question that needs to be considered. It has been suggested that the ability to revoke consent and withdraw from participation is a good indicator of consent being truly free[34]. This is shown in Article 12.4 of the Privacy Code, which states that individuals who have enrolled in a biometric system should be given the opportunity to have their biometric information removed from the system upon request where *possible*. The «possible» criterion might in practice become an obstacle for withdrawal of consent. Furthermore, as far as the author is concerned, it may be more meaningful to provide the individual concerned with «truly equal» alternatives when they decide not to provide biometric data, instead of having to give up the service or not enter into a transaction. These alternatives would adhere to the «no disadvantage principle» in the Australian Privacy Charter which states: «People should not have to pay in order to exercise their rights of privacy described in this Charter (subject to any justifiable exceptions), nor be denied goods or services or offered them on a less preferential basis. The

34 Ibid.

provision of reasonable facilities for the exercise of privacy rights should be a normal operating cost».[35]

Besides the consent and notice problem, the covert collection of biometric data can also be facilitated by the use of radio frequency identification chips (RFID). RFID chips can make the unauthorised collection of various biometric data stored on the card much easier. [36] RFID chips can store and broadcast a great deal of biometric information, which could be used from a distance to identify and track individuals without their knowledge and consent.[37] However, the Australian Passport Act 2005 Sec 47 gives the Minister broad powers to force individuals to carry RFID surveillance devices containing unspecified biometric data.[38] As long as this technology is used it will be very difficult to control the unauthorised collection in practice. The privacy protection afforded by the Privacy Act 1988 will be undermined, as any determination made by the Minister permitting the use and disclosure of biometric information will be likely to fall within the scope of «authorised or required by law» (IPP2.d) or «any law that requires the particular information to be collected» (NPP 1.3(e)) and therefore be exempted from privacy restrictions.[39]

4.2 Unnecessary collection

Biometric data may be unnecessarily collected under the following circumstances:

1. When biometric technology is adopted in various circumstances where no strong verification or identification is needed;
2. When biometric technology is used for identification when only authentication is needed.

35 The Australian Privacy Charter was launched in December 1994. It was developed by a specially formed group that styled itself the Australian Privacy Charter Council (APCC). The Council was established in 1992, under the Chairmanship of Justice Michael Kirby. It aimed to develop a Privacy Charter comprised of principles that would encompass and apply to all forms of privacy and surveillance (i.e., not just information privacy); and to both private and public sector organizations and their clients. Note that the Charter as such is not legally binding. See further the Australian Privacy Charter Council (APCC) (1994).

36 It has been reported that some RFID-enhanced passports are easily cracked, allowing the unauthorised reading of the stored information. See Masnick (2006)

37 American Civil Liberties Union (2004). «Naked Data: How The U.S. Ignored International Concerns and Pushed for Radio Chips In Passports Without Security.» Retrieved 15.02.2010, from http://www.aclu.org/Privacy/Privacy.cfm?ID=17078&c=130//.

38 Sec 47 of the Australian Passport Act 2005 states: «Minister may determine particular methods and technologies «

39 Supra note 23 p.26-60

In the Privacy Act, both IPP 1(b) and NPP 1 require that the collection of personal information should be *necessary to the function and/or activity* of the collectors. The OPC has interpreted «necessary» as when «an organization cannot in practice effectively pursue a legitimate *function or activity* without collecting personal information…» (NPP 1.1). The Biometrics Institute Privacy Code Principle 1.1 largely repeats this same wording. However, by giving the individual the right to have their biometric information removed from the system upon request where *possible* (Principle 12.4), the Code tends to give more control to data subjects over the unnecessary collection of their biometric information, although the wording «necessary» and its explication are a bit controversial.

The necessity provisions in the Privacy Act are fine on their face, but in practice they tend to be easily ignored. There are many examples of biometric applications being used in Australia without any apparent significant censure.[40] Is it reasonable to let the organizations themselves be the sole judge of whether biometric information needs to be collected?

Moreover, to determine what is considered to be *necessary* in the biometric context, the criteria of «cannot in practice *effectively* pursue a legitimate *function or activity*» calls for more clarification. The nebulous wording «effectively» is quite likely to be a good excuse for adopting the putatively strong identification[41] offered by biometrics, and there is no clear standard to decide what should be regarded as «effective.» If the «effectively» requirement is interpreted as «quick» or «convenient,» biometric technology may be likely to fulfil the requirement, especially in many commercial applications. If the interpretation is «security» and «accuracy,» it is still quite likely to fulfil the requirement, especially considering that the organizations themselves are the judges, and given the general misconceptions of what biometric technology offers. However, it is quite doubtful if this is what biometrics can *really* guarantee. In many commercial applications, the accuracy rate and the threshold of acceptance is quite low; hence, the False Acceptance Rate (FAR) is quite high[42]. Therefore it might be dangerous to include the «effectively» criterion when determining the *necessity* of biometric use, unless «effectively» is interpreted as denoting a high degree of actual accuracy and reliability.

40 No cases have come before the OPC or the courts concerning the necessity of using biometric technology.

41 Strong identification here refers to very accurate and reliable identification measure.

42 Mansfield, T. (2001). «Biometric Product Testing Final Report, Report X92A/4009309, Biometric Test Program, UK Government Communications Electronics Security Group.» Retrieved Dec 11, 2007, from http://www.securimetrics.com/articles/gfx/cesg-trials-report.pdf. (no longer accessible)

Since the Privacy Act is intended to provide privacy protection, it is at the least questionable if the effectiveness of the organizations' *functions and activity* ought to be the main standard in deciding what is necessary. Ought not the concern about using biometric technology to be whether or not it is disproportionate to the purpose of collection, not whether it is effective enough to the organization's functions and activities? Although it is true that the «function» concern is also an evaluation factor of «proportionality,» it is important to restrict the concern about «function» and «effectiveness» so that it is not excessive. Take, for instance, a scenario where only authentication is needed and biometric information is collected without any de-identifying measures, which in fact makes identification possible. This would be *unnecessary* to the collection purpose while it could be argued as necessary for *effective functions and activities* of the organizations. Consideration ought to be given to including in the Privacy Act the core principle of minimality as found in the EU Directive Article 6(1)(c), which explicitly require the information being collected should be «non-excessive» in addition to an abstract requirement of «necessary». This helps to ensure that the collection of biometric data is proportionate to the primary purpose and not just for effective functions and activity. When no strong verification and/or identification is needed, other traditional means of verification or identification should be adopted instead of using biometrics.

As mentioned at the beginning of this section, there are generally two practices that result in the unnecessary collection of biometric information. To the extent that necessity should be based on the decision of whether it is necessary for the *purpose* of specific collection, the interpretation might be reformulated as follows:

If an organization cannot in practice effectively pursue a legitimate identification or authentication purpose without collecting the biometric information (e.g., when strong identification is needed and there are no other alternative identification or authentication methods available that can achieve the same purpose), then the information would ordinarily be considered as necessary for the collection purpose. It would not ordinarily be acceptable for an organisation to collect biometric information on the off-chance that the information could become necessary for one of its functions or activities in the future. When biometric information is used only for authentication, privacy-enhancing measures shall be adopted to de-identify the biometric information and render it anonymous or pseudonymous.[43]

43 This is in accordance with NPP 8, and I return to this discussion further below.

If strict control of adopting this controversial technology is ensured from the outset, the risks of using biometrics might be eliminated more effectively.

4.3 Function creep: Secondary use and disclosure

Because of its special nature as relatively unique and health-related,[44] biometric information has great potential for being used and collected elsewhere either as a unique identifier or to disclose private health information. This concern of function creep is at the centre of the debate surrounding the privacy risks of biometric technology.

As previously mentioned, NPP 7 deals with identifiers. It provides that an organization must not adopt as its own identifier one that has been assigned by an agency. Accordingly, NPP 7.1 «prevents an organization from acquiring a particular government assigned identifier from all the individuals with which it deals, and using that identifier to organise personal information it holds and match it with other personal information organized by reference to the same identifier».[45] If biometrics falls within the scope of the definition of «identifier,» this principle will restrict the adoption of a biometric identifier unless for specified purposes;[46] thus, to some extent it will restrict the linking and matching ability of biometrics. Yet as pointed out by the ALRC this regulation still leaves much uncertainty[47]. NPP 7.1 currently prevents only an organization from adopting as its own identifier one that has been assigned by an Australian federal government agency; an agent of that agency acting in the capacity of an agent; or a contracted service provider of an Australian federal government agent. If a biometric identifier is issued by state or territory agencies, it will

44 See supra note 17.

45 Revised Explanatory Memorandum, Privacy Amendment (Private Sector) Bill 2000 (Cth), p. 380.

46 NPP 7 provides four exceptions permitting the adoption of such identifiers.

7.1A «An organisation must not adopt as its own identifier of an individual an identifier of the individual that has been assigned by: (a) an agency; or (b) an agent of an agency acting in its capacity as agent; or

(c) a contracted service provider for a Commonwealth contract acting in its capacity as contracted service provider for that contract. However, sub clause 7.1 does not apply to the adoption by a prescribed organisation of a prescribed identifier in prescribed circumstances.» 7.2 An organisation must not use or disclose an identifier assigned to an individual by an agency, or by an agent or contracted service provider mentioned in subclause 7.1, unless:

(a) the use or disclosure is necessary for the organisation to fulfil its obligations to the agency; or

(b) one or more of paragraphs 2.1(e) to 2.1(h) (inclusive) apply to the use or disclosure; or

(c) the use or disclosure is by a prescribed organisation of a prescribed identifier in prescribed circumstances.

47 Supra note 13 P.1023-1027

not be covered by the current provision. Moreover, although NPP 7 stops the private sector from adopting, using or disclosing Commonwealth government identifiers, it does not address the possibility of the private sector (1) collecting the biometric identifier themselves and developing it as its unique identifier, and (2) collecting the biometric identifier from other private sector actors and linking the collected data for other purposes or using them to track people.

On the other hand, IPPs 9, 10 and 11 place some restrictions on use or disclosure for purposes other than collection of data. The same can be said of NPP2 and the Privacy Code's Principle 2. However, the additional control principle of the Privacy Code stipulates that secondary analysis or function creep of biometric information is not permitted without express free and informed consent (Principle 12.3).

The Privacy Act provides a long list of exceptions to the above-mentioned restrictions on secondary use or disclosure of personal information. The following exceptions are worth mentioning in detail:

1. Consent is gained from the data subjects (NPP 2.1b, IPP 10.1.a)2) The personal information should only be used for relevant purposes. In cases of sensitive information, it should be directly relevant (NPP 2.1.a.i.) and the individual would reasonably expect the organisation to use or disclose the information for the secondary purpose (NPP 2.1.a.ii). However, in IPP 10.1.e it is generally required that the secondary use or disclosure should only be for directly relevant purposes.
2. If the information is health information and the use or disclosure is necessary for research, or the *compilation or analysis of statistics*, it can be disclosed (NPP 2(d)).
3. The use and disclosure for that other purpose is *reasonably necessary* for enforcement of the criminal law or of a law imposing a pecuniary penalty, or for the protection of public revenue (IPP 10.1(d)); IPP 11.1(e) or required or *authorised by or under law* (NPP 2.1(g)).

Consent exception

Consent is only meaningful when it is truly informed and free. When biometric information is involved, a clear notification of the risks for secondary use is of great importance. However, the OPC considers that «consent to the use or disclosure can be expressed or implied» and that «… [i]t may be possible to infer consent from the individual's failure to opt out …»[48] This passive implied consent may weaken the effectiveness of restricting function creep. Neglect of the risks and the irritation of unclear and tedious notices may become the

48 Supra note 11 (1), 2.1(b)

main factors that contribute to «implied» consent. A distinct characteristic of biometric technology is that its application is often accompanied with various potential security and privacy risks and wide misconceptions of its accuracy and security-enhancing capabilities. It is therefore important to consider the extent to which consent for secondary use should be by positive consent – as is stipulated in the Privacy Code's Principle 12.3 – rather than «notice and opt-out». Moreover, this also raises the question whether or not «consent» could be an independent legal basis for any kind of use of personal information. Is it reasonable to allow the inappropriate or unnecessary use of biometric information as long as consent is gained?

Relevant purpose exception

The NPP Guidelines from the OPC describe the term *relevant* as «something that arises in the context of the primary purpose,» and *directly relevant* is defined as «a stronger connection between the use or disclosure and the primary purpose for collection.» Biometric information is generally not accepted as sensitive personal information, although it may be health and genetic-related.[49] Thus it followed that any secondary use and disclosure of biometric information for an indirectly relevant purpose is quite likely to be allowed. But what might be the indirectly relevant purpose of using biometric information? If the biometric information is collected for identification[50] at certain occasions, such as entering the workplace, logging onto a computer system in the office, or entering the workplace dining facilities, would using such information for surveillance be justified as *indirectly relevant*? It could be argued this arises from the primary purpose of security control. The ambiguity of the phrase «the context of primary purpose» in the NPP Guidelines may be further increased if «security» is being accepted as an excuse.

Health information exception

The possible health-related nature of biometric information is one thing that makes its use controversial. There is concern that it might be possible to analyse and extract health information from biometric information. Although it might require significant development of the current biometric systems, the huge potential has raised much anxiety. Should some biometric information be regarded as health information? Although at present biometric information

49 See, e.g., supra note 18. For a discussion on the controversial issue of whether biometric data should be regarded as sensitive personal data, see supra note 17.

50 It is believed that without special privacy enhancing features installed from the outset, biometric information is generally identifiable.

is not treated as health information in general, the potential for doing so is possible. If this happens, will it be reasonable to disclose it for the *compilation or analysis of statistics*? Unlike other health data, which may be more easily anonymised, the relative uniqueness of biometric data and their inherent nature as identifiers make their use relatively problematic. Moreover, the purpose of such *compilation or analysis of statistics* is not restricted in the Privacy Act. This could make function creep to a large extent unavoidable, since tracking and linking might also be justified as involving the *compilation or analysis of statistics*.

Law enforcement exception

Biometric information has a long history of being used in forensic research for purposes of law enforcement. It is, for example, trite that law enforcement agencies use fingerprints and DNA to identify criminals. Hence, biometric information is quite likely to be required for law enforcement purposes. There is much concern that many innocent people's biometric information could be used for such purposes without there being reasonable grounds for suspicion. The long-standing legal doctrine of «innocent until proven guilty» may to some extent be undermined by this use of an individual's biometric information. The nebulous words *law*, *under*, *authorised* may massively expand the scope of the law enforcement exception, as «law» can be understood as federal law, state law, common law, and/or international conventions. The words «under» and «authorises» are also highly subjective and open to debate[51]. The Australian Privacy Foundation pointed out that «it is Exception 2.1 (g) more than any other that undermines the «honesty» of privacy statements and policies which seek to reassure individuals about confidentiality»[52]. A wide range of public agencies will gain enormous power to require disclosure of personal information. In the context of biometrics, function creep in this field becomes almost inevitable.

Summary

The potential of function creep is not likely to be effectively restricted by the Privacy Act or Privacy Code, despite principle 12.3 in the Code. It is reasonable to predict that function creep of biometric information will be inevitable, although it may take some time before it becomes a widespread unique identifier. There is no natural barrier against function creep of this kind: each step can be more or less convincingly justified, and the race to a state of ubiqui-

51 Supra note 5 p.20
52 Ibid.

tous surveillance can run unimpeded.[53] This poses the question of whether it would be necessary to adopt additional legislative measures around the use of biometrics to address the function creep issues.

4.4 Anonymity

Anonymity is an important aspect of privacy. Of special concern is that the application of biometric technologies generally undermines anonymity and pseudonymity[54]. While this concern is not clearly addressed in the IPPs, the NPPs include an anonymity principle (NPP 8) that requires organizations to give individuals the option of not identifying themselves when «entering transactions with an organisation» where it is «lawful and practicable» to have that option. In the Biometrics Institute Privacy Code this principle is essentially repeated (Principle 8), but the supplementary Principle 11.2 suggests that, where practicable, biometric information shall be de-identified by removing the name, thus making it difficult to match with personal information. Privacy impact assessment and auditing are also stipulated in the Code's additional accountability principle (13.2), which could be seen as necessary when adopting privacy-enhancing measures to satisfy NPP 8. In addition, it is likely that the anonymity principle may also be applied to the public sector in the near future, if the ALRC's proposal to that effect is implemented.[55]

The anonymity principle has been regarded as a unique principle of privacy protection that does not occur in the OECD guidelines or the EU Directive. Though De Hert's report mentions the anonymity approach as a good tool for enhancing the opacity of biometrics[56], it does not provide specific legal suggestions regarding how anonymity can be guaranteed in the biometric context.

It has been argued that the anonymity principle in Australian law has failed to live up to its potential as a significant protection device[57]. To comply with this principle in the biometric context, it is necessary to note the following: biometric technology is generally inconsistent with anonymity,[58] though it is

53 Clark, R. (2002). «Biometrics' inadequacies and threats and the need for regulation.» Retrieved 15.02.2010, from http://www.rogerclarke.com/DV/BiomThreats.html .
54 Ibid.
55 Supra note 13 p.693
56 De Hert, P. D. (2005). «Biometrics: Legal issues and implications. Background paper for the Institute of Prospective Technological Studies, DG JRC – Sevilla.» Retrieved 16.02.2010, from http://www.statewatch.org/news/2005/apr/jrc-biometrics-paul-de-hert.pdf.
57 Supra note 31 p.17
58 Supra note 17

possible to use biometric technology for anonymous authentication[59]. It has been stated that if you really want to be anonymous, biometrics is not the appropriate technology of choice.[60] For informatics system generally, unless the anonymising technology is built in at the design stage, it can very likely be claimed as «impractical» to assimilate it in a later stage. The OFPC advises that «NPP 8 has substantial implications for the design of information technology systems»[61], and «additional cost, inconvenience, or administrative inefficiency will not be sufficient grounds for refusing an anonymous transaction»[62]. However, in practice, since a Privacy Impact Assessment is not required under the Privacy Act, and there is no compulsory auditing, it is unlikely that any party will intervene at the design stage, and, as a result, the collector might always be able to claim «impracticability» as an excuse for not offering anonymous use options.

The use of privacy-enhancing technologies to achieve privacy protection through anonymity has been of major interest[63]. This is only mentioned in the draft NPP Guidelines as a possible means to assure anonymity. The Privacy Code clearly encourages it in Section B of the Objective and Principle 11.1 by suggesting the encryption of biometric information immediately after collection. However, the encryption technology is more likely to serve the security purpose better than the anonymity purpose.[64] The listed means in the Privacy Code are somewhat abstract, and given that in many cases the object of biometrics is identification, the possibility of anonymity might seem impossible. It would also not seem to be *practicable* to store the biometric data separately from other personal information. In cases where biometrics can be used for anonymous authentication, it might fail to pass the «necessity» test for collecting such identifiable personal data. However, it is still feasible for biometrics to be applied in a manner that protects identity, if «pseudonymous» options are mandated as an alternative. This has also been proposed by the

59 Grijpink, J. (2001). «Privacy law: Biometric and Privacy.» *Computer law and Security Report,* Vol. 17(3): 154-160. And Impagliazzo, R. and S. M. More (2002). «Anonymous credentials with biometrically-enforced non-transferability.» Retrieved 16.02.2010, from http://portal.acm.org/ft_gateway.cfm?id=1005150&type=pdf&coll=&dl=ACM&CFID=15151515&CFTOKEN=6184618.

60 Interview with Dr Ted Dunstone, Chair of the Biometric Institute in Australia, Sydney, Aug. 2006

61 See Supra note 11

62 Ibid.3

63 Hes, R. and J. Borking (1998). «Privacy Enhancing Technologies: the Path to Anonymity (Revised Edition) Dutch DPA.» *Background studies & Investigations*. Retrieved 16.02.2010, from http://www.dutchdpa.nl/downloads_av/AV11.PDF?refer=true&theme=purple.

64 I will return to this in the following section.

ALRC, which believes that if there is an option for an individual to interact pseudonymously, «it will provide a more flexible application of the principle, by covering the situation where it would be impracticable or unlawful for an individual to transact anonymously but where these barriers would be overcome if the individual were to transact pseudonymously with an agency or organisation»[65]. Bygrave has expressed a similar idea when referring to regulation of profiling by data protection laws generally. He points out that the appropriate rules should stipulate anonymity as the primary goal, with pseudonymity as the first fall-back option when anonymity cannot be achieved for legal or technical reasons. [66] In the scenarios of biometric applications, pseudonymity may be a practical alternative when real anonymity is either impractical or unlawful to implement.

Another weakness of NPP 8 is that it fails to clearly regulate who is supposed to take the responsibility of ensuring anonymity[67]. If the responsibility is in the hands of the collector alone, then the data subject of personal information will likely fall out of any considerations taken when making the decision. Once the disclosing organizations fail to comply with the principle, the indirect collector may be able to claim that since the possibility for anonymity is not built in when the information is disclosed, it would be «impracticable» for it to be built in at a later stage[68]. Without clearly sharing the responsibility of being the disclosing party, this «impracticable» claim is even more likely to remain in the biometrics scenarios.

Concerning the «Privacy Impact Assessment» stipulated by Principles 13.3 and 13.4 of the Privacy Code, it may introduce a process under which due considerations can be given to how the anonymity principle can be respected and made effective. This is a very good process that should be encouraged in general, and not just for the practice of this principle alone. If the Privacy Impact Assessment reveals significant privacy risks, further privacy-enhancing measures should be adopted. Nevertheless, it is worth noting that there is some uncertainty about who is to conduct a Privacy Impact Assessment under Principles 13.3 and 13.4 of the Privacy Code. Principle 13.3 stipulates:

---

65 Supra note 13 P.696

66 Bygrave, L. (2002). *Data Protection Law: Approaching Its Rationale, Logic and Limits' Kluwer Law International*. Hague, London, New York, Kluwer Law International.

67 Clarke, R. (2005). «Submission to the Senate Legal and Constitutional Committee re its Inquiry into the Privacy Act 1988.» Retrieved 15.02.2010, from http://www.rogerclarke.com/DV/SenateReview0502.html.

68 Supra note 23 p.33

A code subscriber must consider «end-to-end» privacy management issues when providing a product or service to an information technology system … this also includes privacy audits, [and] privacy impact assessments …

It is not clear here whether an independent assessor is to conduct the Privacy Impact Assessment as it is suggested for auditing in Principle 13.2, or whether it will be made public what is actually expected to be done in the «Privacy Impact Assessments.» The Privacy Impact Assessment guidelines for public sector agencies developed by the OPC might be a good reference for the implementation[69]. It could also be applicable in the private sector.

4.5 Information security risks and biometrics

Biometric technology has long been utilized as a weapon for combating fraud and providing security; however actually biometrics is no more than an alternative identification or authentication measure. It has its own advantages and disadvantages, and can both solve and cause security problems. The insecurity of storage and transmission, permanent identity theft, and inaccuracy problems are the main security risks raised by biometrics. [70]

Storage

The vast amount of biometric information stored in databases increases the risks of potential identity theft and fraud. Central storage and dissemination in various regions all over the world makes stored personal information vulnerable. In order to reduce the fears of fraud and misuse of personal information, IPP 4 and NPP 4 both require organizations to take reasonable steps to protect the information they hold from misuse and loss, and from unauthorised access, modification, or disclosure. In addition, IPP 4 requires that the personal information be kept in the same manner when it is necessary to give it to a third party. While NPP 4 does not mention the security requirement concerning secondary disclosures, it requires that organisations take reasonable steps to destroy or permanently de-identify personal information if it is no longer needed for any purpose for which the information may be used or disclosed under NPP 2. The Privacy Code repeats almost the same wording as NPP 4. Most of the additional provisions under the new «protection» Principle 11 of

69 Australian Government Office of Privacy Commissioner (2006). «Explanatory Statement Approval of Biometrics Institute Privacy Code.» Retrieved 15.02.2010, from www.privacy.gov.au/business/codes/biometricses.pdf.

70 UK Government Biometrics Working Group (2003). «Biometric Security Concerns.» Retrieved Dec 3, 2006, from http://www.cesg.gov.uk/site/ast/biometrics/media/BiometricSecurityConcerns.pdf (no longer accessible)

the Code are in effect supplementary guidance on compliance with this security principle. Specifically, it requires encryption of biometric data immediately after collection; holding biometric data separately from other personal data; keeping the biometric data in storage only as long as necessary; transmitting the biometric data with «due care;» and limiting access to the biometric data. A similar idea is reemphasised in the ALRC's report suggesting that the best practice for organisations is to hold certain information in an encrypted form, and mentioning biometric information as an example of such information[71].

Both the NPP and IPP guidelines elaborate the definition of *security* as being physical security, computer and network security, communications security, and personnel security. To make this principle practical and effective, the storage of biometric information may need more clarification. For example, it is clear from the legal provisions including the Code that organizations need to take security measures to protect the biometric information stored in their databases. However, it is not clear whether similar requirements should be extended to the biometric information stored in portable tokens such as in the new biometric passport, or any other kind of biometric smart card issued by government agencies or private sector actors. It has been reported that the smart card used to store facial recognition information in the new Australian passport is encrypted by BAC technology.[72] However, the nebulous provisions in law may become a loophole for other biometric applications when biometric information is stored in the issued computer chips, and thus the data recorder does not actually hold them.

The Privacy Code has taken a further step by specifying some security measures. Encryption becomes a mandatory measure to protect the stored biometric data, but it is not clear what strength of encryption is appropriate, and whether there are alternative suggestions. «Separation» storage is suggested for fulfilling the de-identification principle, which is also relevant to NPP 8. However, it is uncertain whether this measure is adequate enough to protect the data, as «destroy or de-identification must be permanent, which means

71 Supra note 29, p.437

72 The International Civil Aviation Organization, which created the international specifications for countries adopting RFID passports, designed specifications for a process called Basic Access Control (BAC). Basic Access Control works as follows: The data on a passport would be stored on an RFID chip in the passport's back folder, but the data would be locked and unavailable to any scanner/reader that doesn't know a secret key or password to unlock the data. To obtain the key, a passport officer would need to physically scan the machine-readable text that is printed on the passport page beneath the photo (this usually includes date of birth, passport number, and expiration date). The reader would then hash the data to create a unique key that could be used to authenticate the reader and unlock the data on the RFID chip.

that an organisation is not able to match the de-identified information with other records to re-establish the identity of people». [73]The OFPC has suggested that they «should provide guidance about the responsibilities that agencies and organisations have under the 'data security' principle. This should include guidance on the manner in which personal information should be destroyed or rendered non-identifiable. This guidance should address both paper-based records and electronic media. It also may be useful for this guidance to refer to relevant standards for information destruction»[74]. This is particularly complicated for digital records such as biometric data, because some systems only allow for simple deletion, which may only change the tag in the system, but still keep the data. This actually makes it possible to get back the *deleted* data. «De-identification» also calls for more clarification, because when it comes to biometric data, simply removing information such as names, addresses, and ID numbers does not necessarily «de-identify» the biometric data. It has been suggested that an accepted industry standard for secure document destruction or de-identification should be established. Otherwise, biometric data may be easily matched with other information and therefore be identifiable again.

The Privacy Code keeps silent as to whether storage of biometric data should be centralized or not. Central storage of biometric data could pose many security risks such as function creep and identity theft. Hence it would be useful to address where the master biometric templates should be stored. Should a portable token be suggested instead of central storage? If central storage is unavoidable, should it be strictly limited and made more secure with more security measures? Another related issue is this: since it has been proved that a raw biometric image may be closely linked to some health information, and since the biometric template is adequate enough for usage, should the raw biometric image be deleted right after the biometric template is created? As has been shown, it is possible to reconstruct the raw biometric image from the biometric template. If some relevant data are available, should it be reasonable to adopt additional security measures to prevent the reconstruction?

In addition, the Privacy Code is somewhat vague with respect to the transmission of biometric data; it mandates that biometric data can only be transmitted in a «prescribed manner, giving due regard to the security of the medium involved» (Principle 11.5) This actually leaves much to the discretionary judgement of the transmitting entity to determine what the «prescribed manner» will be.

73 Supra note 11
74 Office of Privacy Commissioner, Submission PR215, 28 Feb 2007.

Accuracy

Both IPP 8 and NPP 3 require that an organisation must take reasonable steps to ensure that the personal information it collects, uses, or discloses is accurate, complete, and up-to-date. The Privacy Code again simply repeats NPP 3. However, in its additional accountability principle, various measures such as auditing and privacy management are to be adopted.

The accuracy of biometric data has raised much concern. Given that there is no perfect security system and there is always room for errors, it is very important for organizations to try to minimise the error rate and choose an appropriate threshold to keep the right balance between the two rates. The access and correction principle in IPP 3.1, which provides individuals with a general right to access personal information about them, is a necessary measure to ensure the accuracy of the information. Concerning machine-readable biometric information, the ALRC has emphasised: «An expert with the ability to interpret the results of a machine's analysis of biometric information should be made available to an individual seeking to exercise his or her right of access to this type of personal information»[75].

Another major security concern is that biometrics adds a frightening new dimension to identity theft. A widely accepted biometric identifier may facilitate identify theft at one place for all. If this happens, it may have a major impact on an individual's life. NPP 6 and IPP 6 suggest that it is an individual's right to get access to the personal information an agency or organization holds about him or her, and to challenge or alter the result if it is wrong. However, this will often be impractical in the biometrics scenarios. Without special expertise, it would be very difficult to prove if the biometric data stored are wrong or inaccurate; neither can an ordinary person easily prove whether a match is wrong or inaccurate. To combat this problem, additional security measures still need to be explored by the technicians, but first the misconceptions on the accuracy of biometric technology should be avoided, and manual back-up solutions should always be provided. Finally, accuracy-enhancing technology such as «liveness» detection may be recommended.

6.5 Conclusions

With the current focus on privacy protection in Australia and its special provisions about identifiers, the anonymity principle may provide a useful legal basis of privacy protection for the use of biometric technology. However, the protection available is insufficient to deal with all the legal challenges posed

75 supra note 29, p. 436

by the use of biometric information. Several provisions are inconsistent, confusing and/or unclear.

The approach of the Biometric Institute to give guidance on how privacy principles can apply to the collection and use of biometrics is of considerable value. It is of the utmost importance to provide a higher standard in privacy protection in this sensitive area. The Privacy Code has included some good suggestions that need to be further developed in order to be effectively implemented. However, it is somewhat distressing to see that the Privacy Code cannot yet be seen as an effective and adequate measure for better protection of privacy in the biometric context due to its close linkage to the Privacy Act, where adequate legal support is lacking for the clear interpretation and effective implementation of the Code as was pointed out above. The utility of the large-scale repetition of the wording of the NPPs is at the very least questionable. This to some extent weakens the specialities of the Code, and introduces in to the Code many of the weaknesses of the NPPs. In spite of the additional principles, the Code is not obviously technology-specific and seems to be too abstract and nebulous to be a totally effective privacy code intended to deal with a specific technology application. Its voluntary basis and self-regulated nature may in practice render many good improvements ineffective.

Accordingly, changes to the Code need to be made in response to the above inadequacies. The definition of biometrics needs to be further clarified concerning the verification and identification purposes of the biometric technology and the «identifiability» of biometrics in general. The proposal of the ALRC about creating a unified set of privacy principles is also to be supported[76]

- The exemptions for small business and employee records should be deleted so as to provide privacy protection to the customers of small businesses and to employees who have been entered into a biometric system.
- When biometric information is collected, the notice provided by the data collectors should include clear bullet points concerning privacy risks and security risks for adopting biometric technology.
- Consent should be required not only for secondary collection, but also for direct collection unless there are exemptions. Objective criteria need to be specified to exclude certain biometric information from the protection of sensitive information.
- The use of RFID technology, especially when combined with stored biometric data on the RFID chip, should be strictly controlled in legislation.

76 Supra note 13 p.661-666

- Strict legal control of the necessity of collection of biometric information and the use of biometric technology is encouraged. Positive consent should be required instead of passive consent.
- Interpretation is needed for the «indirectly linked usage» with regard to the use of biometric information in particular and the «compilation and analysis of statistics.» Exceptions seem to be very problematic concerning the use of biometric information, calling for further explanations. The exceptions of «authorised by law» need to be reformulated and clarified with special concern given to the use of biometric information in forensic research. Amendments should be made to principle 7 where a loophole exists for private sector actors to use the same unique biometric identifier from other agencies for other identification purposes.
- The anonymity principles need to be amended to clarify that the anonymity obligation should be considered at the beginning of the adoption of a system, especially when biometrics is being utilised.
- Privacy-enhancing technology and Privacy Impact Assessments by an eligible third party should be required.
- It is highly recommended to avoid central storage of biometric information, and where it is unavoidable, additional security measures should be adopted to increase the storage and transmission security.
- Clear requirements for implementing security measures to protect biometric information stored in portable tokens are also indispensable. Liveness detection of biometric information should be obligatory when the biometric identification or authentication would have a significant detrimental impact on an individual's interests.

FORBINDELSER MELLOM RISIKOVURDERING OG RISIKOHÅNDTERING UNDER ET REALISTISK OG ET KONSTRUKTIVISTISK PERSPEKTIV[1]

Herbjørn Andresen

1 Innledning

Temaet for dette essayet er noen trekk ved forbindelsene mellom risiko og håndteringen av risiko. De formene for risiko og risikohåndtering dette omfatter, er det systematiske arbeidet for å vurdere og å håndtere risiko i virksomheter. Dermed faller individuell risikovilje, som for eksempel oppvises om man hopper i fallskjerm eller bruker tohjulssykkel i Oslo sentrum, utenfor. I tråd med avgresningen i Norsk standard, *Krav til risikovurderinger* (NS 5814:2008) faller også økonomisk risiko som følge av forretningsmessige disposisjoner utenfor. Det gjenstår imidlertid svært mange områder som anses å kreve en form for formell risikohåndtering, blant annet arbeidstakeres helse, miljø og sikkerhet, personvernet til en virksomhets kunder og klienter, informasjonssikkerhet, pasientsikkerhet i helsesektoren, terrorbeskyttelse av havner og flyplasser, vern av miljø og naturressurser, matvaretrygghet med mer. Det sentrale fellestrekket ved disse formene for risiko er at risikoskaperen ikke i direkte forstand selv er den som bærer, eller rammes av, risikoen. I mange tilfeller er det å vurdere og å håndtere risiko underlagt en rettslig plikt for virksomhetene. Ofte, men ikke alltid, har denne plikten form av et krav til å etablere internkontrollsystemer. Essayet handler ikke spesifikt om internkontrollregulering som sådan, men trekk fra denne reguleringsformen kan bidra til å gi et bilde av hva slags former for risiko drøftingene gjelder.

For de fleste delene av denne drøftingen er det tilstrekkelig å fremstille vurdering versus håndtering som en enkel dikotomi. Begge sidene av dikotomien blir imidlertid vanligvis beskrevet gjennom en noe mer finmasket inndeling. NS 5814:2008 deler for eksempel inn vurderingene, det å finne frem til risiko, i følgende prosesstrinn: Identifikasjon av farer og uønskede hendelser, analyse av årsaker og sannsynlighet, analyse av konsekvenser, og beskrivelse av risiko.

1 Dette manuskriptet er et essay, innlevert til doktorgradskurs i vitenskapsteori (kurset SVF-8035, Universitet i Tromsø), våren 2010.

Risikohåndteringen er et område som ligger utenfor den nevnte standarden, men man kan abstrahere enkelte fellestrekk fra typiske forskriftsbestemmelser om internkontroll: Generell reduksjon av sannsynligheten for de identifiserte hendelsene, avdekke om noe som burde unngås har skjedd, reagere på hendelser, gjenopprette skader, og lære av det som har skjedd.

Man kan, intuitivt, tenke seg situasjoner der sammenhengen mellom risikovurdering og risikohåndtering blir uklar. Et eksempel er helseinstitusjoners plikt til å varsle Helsetilsynet i fylket om betydelig personskade eller om hendelser som kunne ha ført til betydelig personskade (spesialisthelsetjenesteloven § 3-3), som et lovbestemt tiltak for håndtering av risiko, som står i sammenheng med krav til interne kontrollprosedyrer. Formålet er å avverge, reagere på, og lære av slike situasjoner – tre sentrale aspekter ved risikohåndtering. Denne plikten for helseinstitusjonen forutsetter interne prosedyrer som stiller krav til de ansatte, og innebærer synliggjøring av feil. Selv om en flink institusjon sikkert kan lykkes i å etablere rutiner som ikke fostrer handlingslammelse eller en klandringskultur, er det neppe utenkelig at man av og til, noen steder, håndterer risikoen ved å ty til ryggdekningsstrategier som kan øke faren for at pasienten ikke får den beste behandlingen. Mange sider ved forholdet mellom risikovurderinger og risikohåndtering kan egne seg for empiriske undersøkelser, men i dette essayet er det noen mer fundamentale, teoretiske betraktninger som drøftes.

2 Problemstilling

Betegnelsene vurdering og håndtering antyder en forutsetning om at det normale forløpet vil være en sekvens. Risikoen finnes der ute et sted, og vurderingene går ut på å forstå den, å bestemme seg for hvorvidt det er bryet verdt å avverge den, og å bestemme hva man skal gjøre når en hendelse inntreffer. I det forutsatte normale forløpet blir virksomhetens vurderinger og beslutninger som en stafettpinne, der kunnskap om risiko overleveres til den praktiske håndteringen av risikoen.

Spørsmålet om hva risiko er, herunder om det er en sosial konstruksjon eller ikke, kan drøftes med utgangspunkt i ulike posisjoner. Et ytterpunkt kan betegnes som en naiv realisme. Man bygger da på en forutsetning om at den risikoen som man har analysert seg frem til avspeiler en reell risiko slik den faktisk eksisterer i verden. Dette utgangspunktet ligger til grunn for eksempel hos Starr (1969), i en artikkel som ofte henvises til som et pionerarbeid innen forskning på risiko som grunnlag for policybeslutninger i samfunnet. En alternativ posisjon, som kan sies å representere et klart mer konstruktivistisk perspektiv, går ut på at oppfatninger om hva risiko er, hvordan risikofaktorer

velges ut og hvilken risiko som kan aksepteres, skapes av de preferanser og forventninger som finnes innenfor en kultur (Douglas og Wildavsky, 1982). Den kulturelle teorien har altså klare konstruktivistiske elementer, men den står ikke langt ute på noen radikal, konstruktivistisk fløy. Perspektivet er fremdeles at risikoen er reell, og at det er meningsfullt å håndtere den. Selv om både risiko og risikohåndtering er konstruksjoner, underlagt sine kulturelle og historiske muligheter og begrensninger, er forfatterne opptatt av ikke å bli betraktet som rene relativister:

> *The idea that public perception of risk and its acceptable levels are collective constructs, a bit like language and a bit like aesthetic judgment, is hard to take. The central thesis that the selection of dangers and the choice of social organization run hand in hand goes against the grain of contemporary thought. (…) That perceptions of right and truth depend on cultural categories created along with the social relations they are used for defending has been recognized by a philosophical tradition since the nineteenth century. The more we draw on this tradition, the more we are beset with charges of relativism. (Douglas og Wildavsky, 1982, s. 186)*

Også flere andre innflytelsesrike bidrag til tolkning av risiko, etter Douglas og Wildavsky, har preg av en tilsvarende relativt moderat konstruktivisme, eller en kritisk realisme. Antakelig er det rimelig å plassere beskrivelsen hos Beck (1992), av risikosamfunnet som et sammenvevd nett av teknologiske og sosiale risikodiskurser, som en form for kritisk realisme. Flere er også opptatt av å bygge broer over teknologiske/reduksjonistiske og sosiale/konstruktivistiske perspektiver, som et ønske om « a more organized system for conducting research that takes advantage of the best features of the paradigms competing over claims to risk knowledge.» (Rosa, 1998).

Det å være «relativist» vil i denne sammenhengen kunne ses som en mer radikal, konstruktivistisk posisjon, der risiko ikke tilkjennes noen ontologisk eksistens utenfor språket. En slik posisjon kan for eksempel bygges opp fra Berger og Luckmanns (1967) klassiske teori om hvordan det man tar for gitt blir konstruert gjennom sosial interaksjon, i en prosess der kunnskapen først objektiveres og siden internaliseres. Dette kan man tenke seg som det motsatte ytterpunktet av naiv realisme. Et slikt syn på risiko har antakelig sine talsmenn, som sannsynligvis er i stand til å argumentere godt for standpunktet. Det er imidlertid ikke lett å finne representanter for en relativistisk, radikal konstruktivisme innenfor etablert teori om risiko. Det radikale ytterpunktet ser ut til å befinne seg på utsiden av de etablerte risikodiskursene. Innenfor de ulike diskursene finnes det tross alt en konsensus om et slags essensialistisk risikobe-

grep. Frontene innen risikoteori beveger seg mellom naiv realisme og en klar, men likevel forholdsvis moderat konstruktivisme. Dermed er det tre posisjoner som drøftes i dette essayet, en naiv realisme, en moderat konstruktivisme, og en radikal konstruktivisme. Den siste, radikale posisjonen kan ses som en grunnleggende begrepskritisk betraktningsmåte, et rendyrket utenfraperspektiv.

3 Naiv realisme, et spørsmål om god eller dårlig risikohåndtering

Uttrykket «naiv realisme» kan ses som en positivistisk og instrumentell posisjon, der aktørene tar forbindelsen mellom metodene for og resultatene av risikovurdering og risikohåndtering for gitt. Bakgrunnen for å skrive et essay om risikohåndtering er at jeg har støtt på noen lett brysomme tankekors i arbeidet med et kapittel i min ph.d-avhandling. Kapitlet har overskriften «risikobasert internkontroll som reguleringsmetode». Det som undersøkes i avhandlingskapitlet er virksomheters handlefrihet og samfunnets kontroll med en rekke former for risiko, i lys av bestemmelser om internkontroll i en del lover og forskrifter. Selv om det er en kritisk undersøkelse, er den i hovedsak gjennomført innenfor reguleringens realistiske grunnposisjon.

Selv når man legger en naiv realisme til grunn, er det ikke nødvendigvis sikkert at risikohåndteringen lykkes i å avhjelpe risiko. Det kan også tenkes å gå enda verre, hvis risikohåndteringen er riktig dårlig vil den kanskje bidra til å øke risikoen, eller plassere ansvaret for at noe går galt på feil sted. Vellykket risikohåndtering kan imidlertid læres, hvis velviljen er til stede og det settes av tilstrekkelige ressurser. Naiv realisme betyr ikke at man er «dømt til å lykkes», men at å lykkes eller ikke beror på om risikohåndteringen er god eller dårlig.

Risikohåndtering har i utgangspunktet en utilitaristisk innretning. Selv om det finnes enkelte eksempler på at man går svært langt i å kreve reduksjon av risiko, for eksempel i terrorsikring av flyplasser, er risikohåndteringens logiske mål en nyttemaksimering, ikke risikofrihet. Regnestykkene over nytte gjøres på et akkumulert nivå. Avveiningene mellom mulig skade og samfunnshensyn er systemvurderinger, små avvik blir rettferdiggjort av den overordnede balansen. Den utilitaristiske rettferdiggjøringen av virksomhet som innebærer en risiko kan betegnes som et fortynningsproblem. Det moralsk kritikkverdige tynnes ut når man reduserer sannsynligheten for skader, mens nytteverdien ved virksomheten er konstant (Hansson, 2002).

I generell form er ikke den utilitaristiske innretningen nødvendigvis begrenset til en naiv realismeposisjon. Dersom man trekker det utilitaristiske utgangspunktet litt lenger, kan man imidlertid kanskje si at skillet mellom vurdering og håndtering gjenspeiler et skille mellom «er» og «bør», eller en faktasfære og en verdisfære. Risikohåndteringen får da en normativ side, den

anviser hva rasjonelle aktører *bør* gjøre for å maksimere nytte (Rosa, 1998 s. 20). Å skille ut risikohåndteringen som et mer normativt anliggende enn risikovurderingen, forutsetter en posisjon som ligger relativt nær ytterpunktet naiv realisme. En normativ forståelse ligger også til grunn i den distinksjonen jeg har trukket her mellom god og dårlig risikohåndtering. En vurdering vil ikke på samme måte som håndteringen være god eller dårlig, den vil snarere være riktig eller gal – selv om riktig og gal i denne sammenheng gjerne kan omskrives til godt eller dårlig håndverk. Når risikohåndtering betraktes som en form for normativ konsekvens av vurderingene, betyr det at hva man bør gjøre vil følge «naturlig» dersom man har hatt tilstrekkelig informasjon og har vurdert denne riktig:

> *Organizations and elites who make such decisions, especially in large corporations and federal regulatory agencies, still hew to the line that the problem with risk acceptability is insufficient and low quality information. The normative theory behind this line of thought holds that if only the reality can be ascertained, prescriptions for action will be self evident. (Clarke og Short, 1993 s. 380)*

God risikohåndtering er ikke nødvendigvis begrenset til bare å treffe tiltak som reduserer sannsynligheten for uønskede hendelser. En alternativ strategi er å utbedre skader, lære av dem, og å tilpasse seg til det som forvolder skaden. Wildavsky (1988) analyserer utførlig de alternative strategiene *anticipation* og *resilience*, det å foregripe eller å reparere og tilpasse seg, som idealtypisk forskjellige måter å håndtere risiko på. Disse to universelle strategiene vil finnes i ulike blandingsforhold i alle slags systemer som er gjenstand for risiko. Et resonnement som Wildavsky setter av mye plass til, og eksemplifiserer med ulike typer systemer, er at resiliensstrategier i mange tilfeller gir et tryggere samfunn enn forsiktighetsstrategier. Selv om Wildavsky vanligvis forbindes med retningen kulturell teori og en mer konstruktivistisk tilnærming til risiko, er disse idealtypiske håndteringsstrategiene like velegnet innenfor en realistisk posisjon. En resiliensstrategi kan ses som en direkte motsats til det populære begrepet nulltoleranse: «Political discourses of zero-tolerance sit uneasily with a risk-based ethos.» (Power, 2004 s. 22).

I utgangspunktet er «naiv realisme» en grunnposisjon med et rikt, og ikke naivt, begrepsapparat for håndtering av risiko. Den fører imidlertid også med seg enkelte paradokser, eller i det minste tankekors, som har å gjøre med at det er en posisjon som stiller krav til en relativt klar sekvensiell sammenheng mellom en risiko og håndteringen av den.

3.1 Noen tankekors med utgangspunkt i den realistiske posisjonen

Tankekorsene har opphav i et kapittel om risikobasert regulering i min ph.d-avhandling. I avhandlingskapitlet er disse tankekorsene ikke forfulgt nærmere, fordi fremstillingen der først og fremst dreier seg om å kartlegge virksomhetenes handlingsrom innen denne typen rettslig regulering. Det er tre slike tankekors som drøftes her. Det første, som dreier seg om at forbindelsen mellom vurdering og håndtering kan svikte, er en allmenn teoretisk betraktning. De neste to har mer direkte forbindelse med regulering og risikohåndteringens normative side. Et av disse tankekorsene er at risikohåndteringen foregår innen en virksomhets domene, mens risikoen ikke nødvendigvis kan avgrenses tilsvarende. Det siste tankekorset ligger nærmere en rettsteoretisk distinksjon, hvorvidt en utilitaristisk innrettet normativt føring kan ivareta rettigheter for den som rammes av «uønskede hendelser».

3.2 Risikohåndtering som er koblet fra vurderingene, eksemplet sekundær risiko

For at valget av en bestemt måte å håndtere risiko på skal kunne begrunnes som det beste valget, eller som det en rasjonell aktør bør gjøre, forutsettes det at valget av håndtering er en plausibel konsekvens av risikovurderingen. Dette vil ikke alltid være tilfelle. Michael Power (2004) peker på en fare for at virksomheters ledelse over tid flytter oppmerksomheten fra det han betegner som primær risiko til sekundær risiko. Primær risiko er uønskede hendelser og negative konsekvenser av direkte betydning for det aktuelle samfunnshensynet som risikoen kan ramme. Sekundær risiko er trusselen om sanksjoner eller negative konsekvenser for virksomhetenes omdømme, eller til og med konsekvenser for ledernes personlige renommé, uttelling i et belønningssystem eller videre karrieremuligheter. Særlig i de tilfellene hvor risikohåndteringen foregir å skulle ivareta et bestemt samfunnshensyn, vil det å håndtere sekundær risiko føre til at koblingen mellom vurdering og håndtering svikter.

Risikovurdering av sikkerheten for et nettbanksystem kan tjene som et mulig eksempel på omformulering av en hendelses ugunstige konsekvenser, fra primær til sekundær risiko. Omformuleringen kan være fra «kunden taper penger» til «bankens omdømme svekkes». Dette er ikke nødvendigvis en avdramatisering av konsekvensen. Tvert i mot kan bankens ledelse bli mer skremt av tanken på svekket omdømme, og etterfølgende langsiktige tap, enn av å utsette enkeltkunder for urett eller ubehag. Ut fra en ren kvantitativ vurdering, kan det koste mindre å erstatte noen kunders tapte penger enn å investere i egnede risikoreduserende tiltak. En risikovurdering som omfatter omdømmekonsekvenser kan rette opp denne skjevheten i regnestykket, slik at de risikoreduserende tiltakene likevel lønner seg. I dette enkle, konstruerte

eksemplet bidrar altså oppmerksomhet om en sekundær risiko til bedre konkret risikohåndtering. Man har imidlertid ingen garanti for at opptattheten av sekundær risiko alltid vil forsterke virksomhetens opplevelse av behovet for å ivareta det foregitte samfunnshensynet. For å trekke eksemplet litt videre, kan den samme banken ha kommet til at det er mer lønnsomt å investere direkte i polering av omdømmet enn å investere i risikoreduserende tiltak. Den enkelte kunde løper fortsatt samme risiko for å tape penger, men dersom omdømmestrategien lykkes vil det være færre som finner på å klandre banken for det.

3.3 Institusjonelt innelåst risikohåndtering

Forutsetningen om en sekvensiell sammenheng mellom risikovurdering og risikohåndtering støter også på et slags «territorielt» problem. Den virksomheten som skal håndtere risikoen vil normalt bare ha handlingsevne til å håndtere risiko på avgrensede områder, mens risikobildet endrer seg i takt med forhold som like gjerne befinner seg utenfor det området virksomheten har evne til å håndtere. Med andre ord, i en risikovurdering vil man både identifisere risikofaktorer som man kan påvirke, og risikofaktorer som man ikke kan påvirke.

Behovet for beskyttelsestiltak for en nettbank kan igjen tjene som eksempel. Blant de mange risikofaktorene en bank tar stilling til i sine vurderinger, vil en del av dem handle om faren for at en bedrager, som aldri har oppsøkt banken eller etablert noe kundeforhold, skaffer seg tilgang til en legitim kundes konto. Bedrageren kan forsøke å gjette seg til de passord og øvrige akkreditiver som en kunde har. Banken viktigste håndtering av risikoen vil antakelig være tiltak som reduserer sannsynligheten for dette. Bedrageren kan imidlertid også forsøke å utnytte teknologiske svakheter, som for eksempel kan ha oppstått i en ny versjon av et nettleserprogram. En tredje mulighet bedrageren har, er å stjele fysiske kort og akkreditiver fra kundens postkasse, kontor eller bolig. Både oppgraderinger av nettlesere og en situasjon der politiet må gi oppklaring av postkassetyverier lav prioritet er forhold som ligger utenfor virkefeltet for bankens risikohåndtering. Det hindrer selvfølgelig ikke banken i å treffe tiltak som også omfatter risikofaktorer som endres utenfor bankens kontroll. For eksempel kan de legge lista lavt for å klandre og eventuelt utestenge kunder som banken mistenker for å være uforsiktige. Det har trolig lite for seg om banken skulle prøve å påvirke store internasjonale programvareselskaper eller politiets prioriteringer. Kunden, som er bedragerens målskive, har de derimot innen rekkevidde. Det ligger klart innenfor en realismeposisjon for risikohåndtering å skyve problemet som er identifisert over på kunden, selv om risikovurderingen har synliggjort at problemet egentlig ligger et annet sted. Risikovurderingen peker kanskje på at problemet ligger ett sted, mens

virksomhetens handlingsevne og strategiske valg fører til at belastningene med risikohåndteringen skyves over på andre aktører enn det som det identifiserte problemet tilsier. Sett fra bankens ståsted kan dette være en helt utmerket risikohåndtering, men det strekker antakelsen nevnt ovenfor, om at «prescriptions for action will be self evident», temmelig langt.

3.4 Risikohåndteringens normative side, risikohåndtering versus rettigheter

De formene for risiko som drøftes i dette essayet er primært av det slaget hvor en virksomhet har plikt til å håndtere risiko som rammer andre. På en del slike områder har den som rammes rettigheter. En utilitaristisk nyttemaksimering kan, i hvert fall ved første øyekast, se ut som et stort, grovt og uegnet verktøy for å anvise handlinger som ivaretar konkrete rettigheter. Det vil da ikke bare være risikovurderingene, men også mer mekanistiske, deontiske plikter, som gir opphav til valg av tiltak for risikohåndtering. Virksomhetens handlefrihet er redusert, fordi man også har plikter som tilsier at man handler på en bestemt måte for å innfri den grad av risikofrihet en ekstern part har krav på. Når jeg sier «ved første øyekast», er det fordi det har vært ført gode argumenter for at vurdering og håndtering av risiko i en del sammenhenger kan være velegnet til å innfri rettigheter som ikke motsvares av rent mekanistiske pliktbestemmelser. Ut fra en rettighetstilnærming kan man for eksempel ivareta en rett til vern mot forurensning gjennom en plikt til å rense væske eller gasser som slippes ut i naturen. Rettighetstilnærmingen fanger imidlertid ikke opp hvorvidt det er høy eller lav sannsynlighet for utilsiktet feilfunksjon, som fører til at forurensingen inntreffer likevel. En risikotilnærming har et rikere apparat for å uttrykke feilmarginer og å fange opp unnlatelser, i dette eksemplet at virksomheten unnlater å innføre tiltak som reduserer sannsynligheten for at svikt i renseteknologien fører til miljøskadelige utslipp. Argumentet er fremført slik i en mer elegant og generell form:

> *A rights theory might absolutely prohibit actions when the actor directly intends to expose other individuals to risk, but not those where risk is only a side-effect or further consequence. The second differentiates positive actions from negative actions or omissions. A rights theory might construct absolute rules concerning harm caused by positive acts, but not those resulting from omissions. (Schroeder, 1986 s. 526)*

Dette tredje tankekorset går dermed på et vis i realismeposisjonens favør. Det er mange tungtveiende grunner til at det er rimelig å regne forbindelsen mellom risikovurdering og risikohåndtering som en bedre vei til adekvate tiltak

enn det alternativene, for eksempel en rettighetstilnærming, kan tilby. Likevel gir forholdet mellom utilitaristisk risikohåndtering og fastlagte rettigheter opphav til av og til å kunne tvile på risikohåndteringens normative kapasitet. På områder hvor det er en overlapping mellom det man vurderer som risiko og det som er noens fastlagte rettigheter, kan man vanskelig begrunne *generelt* at risikohåndtering vil sikre et tilstrekkelig vern av rettighetene.

4 Sosialt konstruert risikovurdering og risikohåndtering

Slik dette essayet er lagt opp befinner posisjonen naiv realisme seg i en viss forstand «på tiltalebenken». De problemene jeg peker på ved denne posisjonen går først og fremst ut på at den forutsetter at risikohåndteringen følger sekvensielt og med en grad av nødvendighet fra risikovurderingen. I den sammenheng gjør den naivt realistiske posisjonen seg skyldig i to klassiske vitenskapsteoretiske synder. Den ene er at årsaksmangfoldet blir oversett. En hendelse som er identifisert som en risikofaktor, i en risikovurdering, kan ha årsaker som ikke fanges opp i den systematiske risikohåndteringen. En hendelse kan til og med være både ønsket og velkommen ut fra andre mål og hensyn enn de som førte til at denne hendelsen ble identifisert som en risiko. Produksjon av risikokunnskap må på et eller annet vis ta inn over seg årsaksmangfoldet som problem, selv om det i mange tilfeller kan være vanskelig å ta behørig hensyn til det i praksis. Den andre klassiske dyd som denne posisjonen synder mot, som er mer fremtredende i drøftingen i dette essayet, er at man i overgangen fra vurdering til håndtering slutter fra «er» til «bør». Risikohåndteringen er et normativt program for hva den rasjonelle aktør bør gjøre med en hendelse, forutsatt at vurderingen bak er riktig. Denne litt tvilsomme slutningen vil, i tråd med den kjente spillteoretiske allegorien «fangens dilemma», kunne være kamuflert som et spørsmål om hva som er det mest rasjonelle valget gitt en begrenset mengde informasjon. Det tvilsomme i denne slutningen ligger i at man da enten må sikre at risikohåndteringen er verdinøytral og hevet over alle interessemotsetninger, eller i at man anser riktig og tilstrekkelig informasjon som et magisk medium som i seg selv kan løse verdispørsmål.

I flere brede fremstillinger av hva sosial konstruktivisme er, legges det vekt på å få frem at konstruktivisme er en samlebetegnelse for mange forskjellige perspektiver og posisjoner, som har visse karakteristiske kjennetegn til felles. Vivien Burr innleder sin fremstilling av emnet med fire slike grunnleggende kjennetegn, som hun sier man kan tenke på som «things you would absolutely have to believe in order to be a social constructionist» (Burr, 2003 s. 2). Disse fire kjennetegnene er henholdsvis en kritisk innstilling til kunnskap som tas for gitt, at kunnskaper står i en historisk og kulturell sammenheng, at kunn-

skap opprettholdes av sosiale prosesser, og at kunnskap og sosial handling henger sammen.

I tillegg til disse fire kjennetegnene er det en viktig markør som står sentralt i å skille mellom ulike posisjoner og retninger innenfor konstruktivismen, nemlig spørsmålet om det finnes en essens, en manifest virkelighet, bak de begrepene man konstruerer. Denne siden ved debattene om sosialkonstruktivisme kan ses som en oppgradert versjon av filosofihistoriens universaliestrid (Gundersen, 1984 s. 74-75), spørsmålet om et generelt begrep har en egen eksistens utover å navngi det partikulære. Spørsmålet om risikobegrepets status, hvorvidt risikoen egentlig «eksisterer», er nærliggende å stille når risiko forstås i lys av sosiale konstruksjoner. Et vanlig skille i risikoteori er mellom risikoens ontologiske og epistemiske status, eller mer hverdagslig, mellom oppfattet og faktisk risiko. I risikoteorien ser man ofte oppfattet og faktisk risiko som både likeverdige, like viktige og samtidig eksisterende størrelser. Det anses altså ofte som viktig å ta hensyn til og å forstå begge deler (Shrader-Frechette, 1990). I dette essayet ser jeg likevel oppfattet versus faktisk risiko som tenkte motpoler, fordi det bidrar til å tydeliggjøre noen trekk ved de posisjonene som drøftes.

I spørsmålet om ontologisk status for en konstruktivistisk frembrakt kunnskap om noe i verden, vil det også være et vitenskapsteoretisk interessant spørsmål hvorvidt det foregår en form for tilbakeføring, i dette tilfellet slik at risikohåndteringen influerer oppfatningen av risiko – eller kanskje til og med den faktiske risikoen. En opplagt og nærmest triviell tilbakeføring finner sted når virksomheten lykkes i å lære noe gjennom risikohåndteringen. Ny kunnskap kan bidra til bedre fremtidige vurderinger, slik at usikkerheten reduseres. Det er en annen og mer problematisk form for tilbakeføring som skal undersøkes her: Kan det finnes en utilsiktet og ugunstig tilbakeføring, slik at selv kompetent håndtering ut fra de beste intensjoner bidrar til den risikoen man ønsker å få kontroll med? Stilt slik er dette et spissformulert, og nærmest fortvilende spørsmål. Det ligner på bruk av rusgift for å redusere smerter; løsningen vil etter hvert bli problemet.

I mitt forsøk her på å anvende teori om sosial konstruktivisme på begrepene risikovurdering og risikohåndtering forenkles fremstillingen til to ulike posisjoner, som kan utfordre den naive realismen, henholdsvis en moderat og en radikal konstruktivisme.

4.1 Moderat konstruktivisme, eksemplifisert med kulturell teori om risiko

Moderat konstruktivisme er relativt utbredt innen risikoteori. En av de retninger som har hatt stor innflytelse, og som derfor kan stå som mønstereksempel her, er den som kalles kulturell teori om risiko (Douglas og Wildavsky,

1982). Under denne teorien kan man si at dikotomien mellom vurdering og håndtering av risiko blir opprettholdt. Hva man velger ut som risikofaktorer, og hvordan disse forstås og vurderes, er imidlertid bestemt av den kulturelle og historiske sammenhengen vurderingene står i. Vurderingene er ikke først og fremst riktige eller gale, de er snarere tenkbare og tilgjengelige eller ikke. Risikohåndteringen er på sin side også rammet inn av en sosial organisering. Hvilke typer hendelser man velger å prøve å unngå, eller å gjøre noe med, står i samme kulturelle og historiske kontekst. Denne teorien har hatt en antropologisk innfallsvinkel, som blant annet har omfattet studier av hva de som arbeider med å vurdere og å håndtere risiko faktisk gjør. Blant annet fant Douglas (1992) i en slik studie at de som arbeider med risikovurderinger er opptatt av å presentere dem som vitenskapelige og nøytrale, til tross for at hun fant klare sammenhenger mellom den enkeltes vurderinger og vedkommendes verdier og faglige og politiske ståsted.

Innen kulturell teori om risiko betraktes ikke håndtering av risiko som en enveiskjørt følge av vurderingene. Det er en dynamikk basert på gjensidighet mellom vurdering og håndtering. En nøkkel til å forstå dette samspillet kan man finne i anerkjente metoder for å vurdere risiko, for eksempel de som er beskrevet i NS 5814:2008. I svært mange tilfeller vurderes ikke risiko ved at man kan gå ut og «lese verden» direkte. Metodene for å vurdere risiko baseres ofte på workshops eller lignede aktiviteter, der antatt relevante interessenter og eksperter drøfter og eventuelt forhandler seg frem til vurderingenes innhold. Sismondo anser det forhold at kunnskap blir til i en type prosess der man også gjerne kunne ha fått andre kunnskaper som resultat i stedet, som et slags intuitivt belegg for konstruktivisme: «The intuition is that It could easily have been otherwise. » (Sismondo, 1993 s. 536). Basert på dette resonnementet, kan man si at handlingene som utgjør en risikovurdering i seg selv blir et belegg for en konstruktivistisk forståelse, fordi det er opplagt at de samme vurderingsaktivitetene også kunne ha gitt andre vurderinger som resultat. Like viktig er det imidlertid at vurderingene er aktiviteter som i stor grad utføres av de samme personene som skal treffe beslutninger om håndtering. Derfor vil vurderingene av risiko ha mulige håndteringsstrategier med som en del av vurderingenes innhold. Burr beskriver «fokus på prosess» som et av de momentene der konstruktivisme skiller seg fra mer tradisjonell forståelse av vitenskapelig kunnskap: «Knowledge is therefore seen not as something that a person has or doesn t have, but as something that people do together.» (Burr, 2003 s. 9). Man kan si at risikokunnskap er noe som eksisterer fordi man gjør risikovurderinger. Samtidig har man innen kulturell teori en essensialistisk forståelse av risiko, men forståelsen av den er filtrert gjennom de rammene som styrer utvelgelsen av og synet på hvilke hendelser som er uønskede.

Spørsmålet om hvorvidt risikohåndtering kan skape risiko blir vanskelig å besvare teoretisk. Det skjer en gjensidig påvirkning mellom oppfatningen av risiko og den organisering og de virkemidler man ellers har for å håndtere risikoen. Derfor skulle man anta at den risiko som man ikke har lært seg å oppfatte, og ikke allerede er enige om å behandle, faller utenfor synsfeltet. Utgangspunktet burde derfor være at risikohåndteringen i liten grad evner å produsere ny risiko utover den man allerede er enige om at det er behov for å håndtere. Det er likevel ikke utenkelig at det på et tidspunkt blir kulturelt mulig å oppfatte nye forhold som risikomomenter, samtidig som risikohåndteringen henger fast i en foreldet organisering tilpasset en delvis utdatert risikokunnskap. I slike situasjoner kan man neppe utelukke at risikohåndteringen bidrar til å øke risikoen.

4.2 Radikal konstruktivisme

Som nevnt tidligere vil man ikke så lett finne radikal konstruktivisme som en tydelig posisjon innenfor etablert risikoteori. Det er derfor fremstilt her som en tenkt posisjon, et utenfra-blikk, basert på mer generelle vitenskapsteoretiske bidrag. Jeg henter momenter fra to i utgangspunktet relativt forskjellige teoretiske bidrag, det ene er Michel Foucaults diskursbegrep, det andre er Bruno Latour og Steve Woolgars studie *Laboratory Life: The Construction of Scientific Facts*. Jeg har imidlertid kun belaget meg på sekundærlitteratur, og henviser til andres filtrerte og fortolkete versjoner av disse bidragene.

Latour og Woolgar undersøkte hvordan vitenskapelig arbeid i laboratorier foregår, og kom til at de naturvitenskapelige fakta ble gyldig kunnskap gjennom en egen, vitenskapelig diskursiv interaksjon. Resultatene er fabrikasjoner, ikke oppdagelser. Sismondo (1993) velger, som han sier, å ta Latour og Woolgars radikale konstruktivisme bokstavelig. Deres arbeid tas som eksempel på den mest radikale posisjonen, det materielle er en transformasjon av det sosialt konstruerte, objektene som er forsket frem i laboratoriet er skapt av en forhandling som har ledet til konsensus. Prosessen er, slik den gjengis av Sismondo, likefrem og forståelig. Likevel anser han den som lite plausibel og svakt begrunnet. I en noe skarpere polemikk mot denne beskrivelsen av laboratoriearbeidets resultater, som fabrikasjoner, skriver Hellesnes (2001 s. 137): «At det faktisk forheld seg slik i kroppen som Guillemin har påvist blir for Latour og Woolgar nærmast ein vits.»

Når Latour og Woolgars fabrikasjonstese overføres til en risikodiskurs, vil det i utgangspunktet være like nærliggende å spørre om *vurderingene* skaper risiko som å stille spørsmålet slik jeg har gjort, altså om risiko*håndteringen* kan ha den virkningen. Både vurdering og håndtering er fabrikasjonsprosesser der ri-

sikoen oppstår, blir begrepsfestet, og eventuelt blir reell. Fabrikasjonsprosessen kan vanskelig oppebære noe normativt prosjekt. Det vil strengt tatt kunne være noe vanskelig å argumentere for at risikohåndtering tjener noe formål i det hele tatt. Hvis laboratorieforskning handler om prestisje og kredibilitet, kunne man kanskje også tenke seg at arbeid med risiko i virksomheter er en form for virksomhetsintern imperiebygging. At det kan finnes elementer av den slags motivasjon også i utbredelsen av risikobaserte kontrollaktiviteter i virksomheter har vært antydet, som i en leges observasjon av at de eneste som likte denne nye formen for styringsinstrumenter var «konsulentfirmaene og kursholderne og endel sersjanter i systemet som ser en karrieremulighet» (Lundevall, 1996).

Om man ser etter mulige motivasjoner for risikovurdering og risikohåndtering, i en situasjon der det man egentlig gjør er selv å fabrikkere det man vurderer og håndterer, begynner man å nærme seg et foucaultsk diskursbegrep. Burr siterer følgende definisjon, fra Foucaults *The Archaeology of Knowledge*: «Discourses are practices which form the objects of which they speak .» (Burr, 2003 s. 64). Ut fra dette perspektivet vil det knapt være mulig, i hvert fall lite fruktbart, for den som betrakter diskursen utenfra å prøve å tillegge risikohåndtering en mer normativ rolle enn vurderingene. Først og fremst er begge deler del av den samme diskursen. Burr anviser følgende kriterium for å avgjøre hva som tilhører samme diskurs: «Pieces of speech or writing can be said to belong to the same discourse to the extent that they are painting the same general picture of the object in question.» (Burr, 2003 s. 66).

Når risikodiskursen ikke lenger gjør det mulig å skille ut risikohåndtering som en normativ konsekvens av vurderingene, altså som en anvisning av hva den rasjonelle aktør bør gjøre, blir det nærliggende å betrakte også nytteverdien av risikohåndtering som en slags fabrikasjon. I så fall ligner risikohåndtering mer på ideologiproduksjon i marxistisk forstand, et instrument for å generere falsk bevissthet som kamuflerer maktskjevhet. Ideologibegrepet er treffende fordi aktørene som bidrar i risikodiskursen verken kan eller vil se det slik. Aktørene gjør simpelthen ting som er mulig innenfor risikodiskursen, og disse tingene er å bidra til konstruksjonene som opprettholder diskursen.

Mens Latour og Woolgar forklarer forholdet mellom konstruksjonsprosessen og resultatene som en slags transformasjon fra det sosiale til det materielle, handler Foucaults diskursteori om at det som konstrueres bare er tilgjengelig innenfor diskursen. Burr betegner dette som at spørsmålet om ontologisk status settes i parentes: «In a sense, Foucault brackets off the question of reality. Since we can never have direct access to a reality beyond discourse we cannot concern ourselves with its nature.» (Burr, 2003 s. 90). Anvendt på en risikodiskurs, vil det si at det eneste vi kan analysere og håndtere er oppfatninger om risiko.

I en foucaultsk, radikal konstruktivisme får spørsmålet om hvorvidt risikohåndtering skaper risiko et litt annet svar enn både i moderat konstruktivisme og i Latour og Woolgars versjon av radikal konstruktivisme. I det foucaultske perspektivet er det nærmest selvfølgelig at oppfattet risiko vil øke i takt med at diskursen vokser seg stor og fet og vinner hegemoni. Uten vekst i den oppfattede risikoen vil man måtte regne med at utbredelsen av risikodiskursen også gikk tilbake. Om en såkalt faktisk risiko også øker i takt med oppfattet risiko, er imidlertid et spørsmål som ikke kan besvares fra denne posisjonen. Problemet med at faktisk risiko er utilgjengelig er imidlertid ikke det eneste som gjør det vanskelig å svare på om risikohåndtering skaper risiko. Vanskeligheten skyldes også at man innenfor en risikodiskurs ikke sitter med overbevisende argumenter for at man bør velge én måte å håndtere risiko på fremfor en annen.

5 En forenklet sammenlikning av de tre posisjonene

Ovenfor har jeg fremstilt tre ulike posisjoner, som er en kraftig forenkling av en rekke måter å se på risiko og risikohåndtering. Den første av de tre posisjonene er naiv realisme, som er utgangsposisjonen. De to andre er henholdsvis moderat og radikal konstruktivisme. De sentrale parameterne for sammenlikning er vurdering og håndtering av risiko, under hver av disse posisjonene. Ved siden av disse to hovedparameterne har drøftingen også ført til en problematisering av sammenhengen mellom vurdering og håndtering i hver av de tre posisjonene. De to siste kolonnene i tabellen sammenlikner risikoens ontologiske og epistemiske status under de ulike posisjonene.

	Vurdering av risiko	Håndtering av risiko	Sammenhenger mellom vurdering og håndtering	Risikoens epistemiske status	Risikoens ontologiske status
Naiv realisme (utgangspunkt i min avhandling)	Riktige eller gale vurderinger	God eller dårlig håndtering	Håndtering er en normativ fordring, direkte basert på vurderingene	«pedagogisk utfordring», kunnskapen kan være rett eller gal	Eksisterer, og er i samsvar med resultatene av riktige vurderinger
Moderat konstruktivisme (Cultural theory som eksempel)	Kulturelt bestemt utvelgelse	Bestemmes av den sosiale organiseringen	Gjensidig påvirkning	Oppfatninger som er påvirket av kulturelt bestemte rammer	Eksisterer som (kulturelt influerte) beslutninger
Radikal konstruktivisme (kritisk blikk, utenfra risikoteorien)	Sosial konstruksjon	Sosial konstruksjon	Er del av samme diskurs, vanskelig å holde fra hverandre	Oppfatningene er den eneste kunnskapen vi kan ha	Utilgjengelig («settes i parentes»)

6 Konklusjon

Problemstillingens utgangspunkt har her vært å se på noen vanskeligheter man støter på ved å betrakte risikohåndtering fra en realismeposisjon. Konstruktivistiske perspektiver har spilt rollen som alternativ innfallsvinkel. Jeg finner at konstruktivistiske perspektiver et stykke på vei bidrar til forklaring og forståelse av disse tankekorsene. Det viktigste bidraget fra det konstruktivistiske perspektivet i denne sammenhengen er at det gir grunnlag for å stille spørsmål ved hvor godt det er mulig for systematisk risikohåndtering å dekke den risikoen som man har analysert seg frem til – i tillegg til at det selvfølgelig, uansett perspektiv, er en fare for at relevant risiko unnslipper fra analysen. Et annet, viktig bidrag fra det konstruktivistiske perspektivet, er at det begrunner en sterk tvil om hvorvidt risikohåndtering er i stand til å oppebære et normativt program, som anviser hva forutsetningsvis rasjonelle aktører bør gjøre.

7 Litteraturliste

Spesialisthelsetjenesteloven. Lov om spesialisthelsetjenesten m.m., lov 2. juli 1999 nr. 61.

NS 5814:2008. «Krav til risikovurderinger». Standard Norge, Lysaker.

Beck, Ulrich (1992) *Risk society: towards a new modernity.* London: Sage.

Berger, Peter L. og Thomas Luckmann (1967) *The social construction of reality: a treatise in the sociology of knowledge*. London: Penguin.

Burr, Vivien (2003) *Social constructionism*. London: Routledge.

Clarke, Lee og James F. Short, Jr. (1993) «Social Organization and Risk: Some Current Controversies». I: *Annual Review of Sociology,* årg. 19, s. 375-399.

Douglas, Mary (1992) *Risk and Blame: Essays in Cultural Theory.* London: Routledge.

Douglas, Mary og Aaron Wildavsky (1982) *Risk and culture: an essay on the selection of technical and environmental dangers*. Berkeley, CA: University of California Press.

Gundersen, Jan Brage (1984) *Den lille filosofihistorien: en nøkkel til filosofiens og vitenskapens historie.* Oslo: Aventura.

Hansson, Sven Ove (2002) «Kan moralfilosofin hantera riskproblemen?». I: Åsa Boholm, m. fl. (Red.) *Osäkerhetens horisonter. Kulturella och etiska perspektiv på samhällets riskfrågor* Nora: Nya Doxa.

Hellesnes, Jon (2001) «Sosial konstruktivisme i vitskapsteorien». I: *Nytt norsk tidsskrift,* årg. 17, nr. 2, s. 132-149.

Lundevall, Sverre (1996) «Om den store lydighetskampanjen som ruller over landet». I: *Utposten,* årg. 25, nr. 7/8, s. 28-31.

Power, Michael (2004) *The Risk Management of Everything: Rethinking the Politics of Uncertainty.* London: Demos.

Rosa, Eugene A. (1998) «Metatheoretical foundations for post-normal risk». I: *Journal of Risk Research,* årg. 1, nr. 1, s. 15-44.

Schroeder, Christopher H. (1986) «Rights against Risks». I: *Columbia Law Review,* årg. 86, nr. 3, s. 495-562.

Shrader-Frechette, Kristin S. (1990) «Perceived risks versus actual risks: Managing hazards through negotiation». I: *Risk,* årg. 1, s. 341-363.

Sismondo, Sergio (1993) «Some Social Constructions». I: *Social Studies of Science,* årg. 23, nr. 3, s. 515-553.

Starr, Chauncey (1969) «Social Benefit versus Technological Risk». I: *Science,* årg. 165, nr. 3899, s. 1232-1238.

Wildavsky, Aaron (1988) *Searching for safety.* New Brunswick, N.J.: Transaction Books.

SCENARIO STUDY OF BIOMETRIC SYSTEMS AT BORDERS[1]

Yue Liu

Abstract

This paper examines and compares the existing privacy instruments of VIS and USVISIT systems in addressing the specific legal issues and challenging the privacy-invasive behaviour in the world of biometrics. A biometric scenario is presented to give a vision of a future society in five years from now when biometric technology is more widely used. The objective here is to open up the scope of considering the potential legal risks of the use of biometrics, based upon the present passport and visa application plans in the EU and USA.

Key Words

biometric, VIS system, USVIST System, privacy, scenario

1 Introduction

This paper examines and compares the existing privacy instruments of VIS and USVISIT systems in addressing the specific legal issues and challenging the privacy-invasive behaviour in the world of biometrics. A biometric scenario is presented to give a vision of a future society in five years from now when biometric technology is more widely used. The scenario is designed to encompass key legal issues for the introduction of biometrics in the border-control environment, which is dominated by public sector actors.

The specific examples are to a large extent illustrative rather than predictive, and the scenarios are by no means all-encompassing. Apart from AFIS (Automated Fingerprint Identification System), a system that has been in use already for many years by police forces in the forensic domain, most of the envisaged applications are too new to be thoroughly tested through daily use at the moment. The objective here is to open up the scope of considering the

1 Paper submitted to The Fifth International Conference on Legal, Security and Privacy Issues in IT Law (LSPI), Barcelona, 3.-5.november 2010.

potential legal risks of the use of biometrics, based upon the present passport and visa application plans in the EU and USA. The VIS (Visa Information System) and US-VISIT (United States Visitor and Immigrant Status Indicator Technology) systems – explained further below – are used as implementation examples of biometric usage, using the scenario as a platform to envisage and compare how and to what extent the legal concerns relevant to privacy might be resolved.

2 Biometric systems at the border

2.1 Visa Information System (VIS)

The EU Council adopted on 8 June 2004 Council Decision 2004/512/EC establishing the Visa Information System (VIS).[2] The Decision (hereinafter also termed «VIS Decision») constitutes the legal basis for the budgeting, development and design of VIS. This is a system built up for the exchange of visa data between EU Member States. It represents one of the key initiatives within the EU aimed at supporting stability and security. The VIS will record the biometric identifiers of visa applicants; this is in order to improve the exchange of information between countries and national border control agencies. The VIS is based on a centralised architecture and consists of a central information system, the «Central Visa Information System» (CS-VIS), and an interface in each Member State, the «National Interface» (NI-VIS), which provides the connection to the relevant central national authority of the respective Member State, and the communication infrastructure between the Central Visa Information System and the National Interfaces. The VIS will store data on up to 70 million people concerning visas for visits to or transit through the Schengen Area. These data will include the applicant's photograph and their ten fingerprints.

The VIS Decision has subsequently been supplemented by Regulation 767/2008/EC concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas (VIS Regulation).[3] The objectives of this Regulation (hereinafter also termed «VIS Regulation») are to define the purpose, functionalities and responsibilities for the VIS, to give to the Commission the mandate to set up and maintain the VIS and to establish the procedures and conditions for the exchange of data between Member States on short-stay visa applications to facilitate the examination of such

2 OJ L 213 of 15.06.2004, p. 5.
3 OJ L 218, 13.8.2008, p. 60–81.

applications and the related decisions. The scope of the Regulation is related to the exchange of data on Schengen short-stay visas as the primary purpose of the VIS, including the national long-stay visas which are concurrently valid as short-stay visas.

2.2 US-VISIT

The United States Visitor and Immigrant Status Indicator Technology (US-VISIT) Program is an integrated, automated, biometric entry-exit system for recording the arrival and departure of aliens (defined as any person who is not a citizen including lawful permanent residents of the United States).[4] The system conducts certain terrorist, criminal, and immigration violation checks on aliens; in addition it uses the biometric identifiers to authenticate the identity of those collected on previous encounters (U.S. Department of Homeland Security 2006, p. 1). It receives all biometric (fingerprints and photographs) and biographic data from the USCIS (United States Citizenship and Immigration Service) ISRS (Image Storage and Retrieval System)/BSS (Biometric Storage System).[5] Data from ISRS/BSS are transmitted to the Automated Biometric Identification System (IDENT), the biometric repository used by US-VISIT, through a direct, secure encrypted connection created between USCIS ISRS/BSS and IDENT.

The US Congress first mandated that the former Immigration and Naturalization Service (INS) implement an automated entry-exit data system to track arrivals and departures of every alien under §110 of the Illegal Immigration Reform and Immigrant Responsibility Act of 1996 (IIRIRA) (Seghetti and Viña 2005, p. 5). There are five principal laws that extend and refine §110 of IIRIRA, namely the INS Data Management Improvement Act (DMIA),[6] the Visa Waiver Permanent Program Act (VWPPA),[7] the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA PATRIOT),[8] the Enhanced Border Security

4 US-VISIT Final Rule: Enrolment of Additional Aliens, Additional Biometric Data and Expansion to More Land Ports, last visited 03.02.2009

5 ISRS/BSS is a USCIS (United States Citizenship and Immigration Service) system that enables users to query the repository of biometric, biographic and card issuance information used to produce Permanent Resident Cards, Employment Authorization Document cards, Border Crossing Cards, Re-entry Permits, and Refugee Travel Documents. See U.S. Department of Homeland Security (2006)

6 Public Law 106-215.

7 Public Law 106-396.

8 Public Law 107-56.

and Visa Entry Reform Act (Border Security Act),[9] and the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTRA).[10] According to the requirements of the relevant provisions in the six above laws, an integrated, automated entry and exit data system that includes the use of biometric identifiers needs to be implemented. That system is the US-VISIT system.[11]

2.3 Scenario

In the near future, Ann, a sales consultant in the marketing department of a company, is going to make a business trip from country N to country F.

Visa application

Ann has been to the embassy of F to get a visa. The visa application involved having several of her fingerprints scanned. She wondered if her fingerprints will be matched against a watch-list of risk persons. But at the embassy no one told her why fingerprints are collected, and how they will be used or stored. There is no notice or announcement posted anywhere in the embassy. She was a bit reluctant to give them her fingerprints, but since it seems to be compulsory for getting a visa, she had no choice. She also saw another man who seemed to have some problem in getting his fingerprint recognised by the device, still trying to get an acceptable fingerprint at the embassy when she was leaving.

She had thought that her fingerprints would be used to authenticate her identity when she arrived in F. This seemed to be the purpose last time when data on both her iris and face were collected for entering another country U. However, this time, when entering F, the fingerprints are not used. It seems they have been collected for some unknown reason. She wonders who is actually using this information and for what purposes.

She sees that, with all her travels, her passport is getting physically thicker. This is due to the inclusion of an increasing number of «contact-less» smart chips in which her biometric data are saved. On her last trip to country R, she had her retina scanned. On the trip before that, to country M in Asia, she had to have another fingerprint scanned for the visa, since M's officials claimed that the extant fingerprint in her passport might not be readable by the sensors of their border-control system.

9 Public Law 107-173.
10 Public Law 108-458.
11 For more information about the legislative history of US-VISIT, see Seghetti and Viña (2005)

N country airport

Ann arrives at the airport 2 hours prior to her scheduled departure. Her personal data and fingerprint information are already collected and registered through on-line booking channels. It is said that the airport can link up to the official central database of all the travellers' fingerprints, facial image and other personal data which can undertake automatic risk analysis by the authorities in advance.

She is allowed to use the green channel as a frequent «good faith» traveller. This channel utilizes a self-service facial-image identification system and her electronic visa to check her in automatically. This is instead of the normal blue channel. (The blue channel is supervised by security guards and usually involves a long time for waiting because false rejections of facial images occur from time to time, and some people do not have sufficiently neutral facial images, and some handicapped persons' wheelchairs are too bulky for them to get close to the facial image monitor. Quite a few people need to go to back-up security for checking of their fingerprint. That means another queue.)

Ann wonders about the red channel, which is used for people who are registered by the authorities as high-risk persons when they book a flight: What kind of security check do they go through? And how exactly do they get marked out as high risk?

She is quite familiar with the green channel system now, though in the beginning it caused her some troubles. Now she simply stands still for several seconds in front of a monitor in a well-lit setting, with a neutral expression on her face. She then inserts in a machine adjacent to the monitor the page of her passport with the chip containing her facial, fingerprint and other personal data. She is then required to enter her flight number followed by a six-digit PIN-code that she has been given and requested to memorise by the passport agency. It is only in the last year that such PIN-codes have been issued; they came as a response to concerns about hacking of the passport chip containing biometric data. Ann's identity is verified, her flight is confirmed, she chooses her seating in the plane, and is issued with her boarding card. The whole process takes a few minutes.

As always, there is a long queue before the checkpoint for boarding the plane, but no biometric is needed at this stage and the queue moves fairly smoothly. Ann gets through without mishap.

Return to N country airport

After having spent 3 hectic weeks in various cities of F, Ann flies back to N feeling rather tired. Shortly after presenting her face before the monitor in the security control system, she is stopped by security personnel and asked to accompany them. She is then walked briskly to a nearby office. The door is opened and awaiting her are two medical personnel with mouth masks.

3 Scenario analysis and comparative discussion

3.1 Notice

When applying for a visa, Ann's biometric data are collected without any kind of notice. This happens quite often nowadays during visa applications to the United States and the UK when fingerprints are collected.[12] Both the VIS[13] and US-VISIT systems make it mandatory to collect biometric information from the visa applicants except for limited exceptions. Article 37 of the VIS Regulation requires the Member States responsible to provide the persons concerned with information on the identity of the controller responsible for the processing, the purposes for which the data will be processed within the VIS, the recipients of the data and the existence of the right of access to, and the right to rectify, the data. This is in accordance with the transparency principle in the European Data Protection Directive, which is regarded as a core privacy protection principle in most legal instruments on data protection. In Articles 10 and 11 of the Directive it is explicitly stipulated that the data subject has the right to be informed when his/her personal data are being processed. The controllers must provide information on their name and address, the purpose of processing, the recipients of the data and all other information required to ensure the processing is fair. However, these requirements seem not to be well implemented in this scenario (and, indeed, in reality).[14]

12 This is according to the author's personal experience at the British Embassy in Oslo, in 2007, and American Embassy in Oslo in 2006.

13 The UK is not part of VIS, but fingerprinting is needed for obtaining a visa to the UK.

14 This is according to the author's personal experience at the British Embassy in Oslo, in 2007.

Although there are no specific provisions or regulations about this notice requirement for collecting biometric information in the US-VISIT program, the US Privacy Act of 1974 limits federal agencies' collection, use and disclosure of personal information, such as fingerprints and photographs.[15] However, the Act grants rights only to US citizens and to aliens lawfully admitted for permanent residence. US-VISIT will inevitably collect information on some number of foreign nationals who will eventually become lawful permanent residents and US citizens. Information about those individuals maintained within US-VISIT eventually will become subject to Privacy Act protection. Accordingly, the Privacy Act covers federal agency's use of personal biometric information of this category of individuals but not in advance of these persons becoming citizens. Subsection e(4) of the Act also requires «notice» of the name and location of the system; the title and business address of the agency official who is responsible for the system of records, the purpose of collection and the way the personal records are going to be used and kept. However, the Act includes exemptions for law enforcement and national security purposes. This broad exemption, provides no guidance on the extent of the appropriate uses law enforcement may make of biometric information. Here it also could be a possible excuse for not giving any notice for this collection. On the other hand, a non-resident foreign national cannot use the Act's provisions. Although a foreign national may use the Freedom of Information Act of 1966[16] to request records about him or herself, it is not clear what kind of privacy protection will be otherwise available for them in practice as the Privacy Act does not cover them.

Creating a legal basis for mandatory biometric information collection has a significant impact on the privacy of the individuals concerned; it should be guaranteed that such collection cannot be implemented without providing the appropriate transparency and legal procedure.

3.2 Exemption from fingerprinting

In the scenario a man with a skin problem is trying to enrol his fingerprints; this illustrates the issue of the categories of persons exempted from the obligation to provide fingerprints or other biometric information. A significant number of persons are said to be unable to enrol into one or more biometric systems. This needs to be borne in mind when a biometric system is created,

15 5 USC § 552a.

16 5 USC § 552 generally provides that any person has the right to request access to federal agency records or information.

as it relates to the accuracy of the data collected and the non-discrimination concerns. The admissibility of the fingerprinting and other forms of biometrics, such as facial recognition, should be discussed in light of the purpose of the biometric system itself. Biometrics will be used for either authentication or identification, and it needs to be judged by an expert whether a biometric identifier is suitable for the purpose. For instance, fingerprints of children below 14 are usually seen as reliable for verification only (European Data Protection Supervisor 2006a, p. 4).

In the US-VISIT program, exceptions are made for children under the age of 14 and persons over the age of 79.(Department of Homeland Security 2009) However, there seem to be no specific exceptions made for persons for whom fingerprinting is «physically impossible». However, this category of person might possibly be treated as «classes of aliens the Secretary of Homeland Security and the Secretary of State jointly determine shall be exempt, or (v) an individual alien the Secretary of Homeland Security, the Secretary of State or the Director of Central Intelligence determines shall be exempt» (Department of Homeland Security 2004). The problem with such a provision is the uncertainty and complexity during implementation, unless there is an additional specific list of exceptions published by the Secretary of Homeland Security and the Secretary of State jointly. The US government's choice of not including the specific exemption list in the same basic text as the one establishing the US-VISIT system seems a bit problematic, considering the importance of the measure and its potential impact on the category of persons who are physically unable to present fingerprints.

Compared with the US-VISIT regulation about children under age 14, the VIS system chooses to only exempt children under age 12 for fingerprinting.[17] This might be problematic too; as the European EDPS states, a generalized fingerprinting of children cannot be seen as a mere technicality and should require a serious democratic debate in the appropriate institutions (European Data Protection Supervisor 2006b). Moreover, another biometric identifier, facial imaging of children may be even more problematic than fingerprints. No age limit on facial recognition is found in the VIS Regulation However, the facial image of a child may change dramatically in just a few years' time; even if the technology of facial recognition makes significant progress, it is unlikely that the software will be able to compensate for the effect of growth on children's face even in a few years' time (European Data Protection Supervisor 2006 b).

17 See Article 13(7) (a) of Regulation 810/2009/EC of the European Parliament and of the Council, establishing a Community Code on Visas (OJ L 131, 28.05.2009).

Hence it needs to be questioned: to what extent are children's facial images useful for identification or authentication? What are the fall-back procedures?

3.3 Access and use limitation

In the scenario, Ann's fingerprints are not collected for authentication; instead, they might be used for identification, or further linking or tracking with law enforcement or other relevant agencies, or just saved for *possible* use in the future.

In the European context, the VIS system establishes links with other applications possibly submitted by the same individual and already recorded in the VIS as well as with the data of individuals travelling in a group in the EU countries requiring the visas.[18] Alphanumerical data of the applicant and on the visas photograph and fingerprint data, links to other applications are all to be stored in the VIS.[19] When it comes to access of this database, the Commission states:

> *In relation to the objective of combating terrorism and crime, the council now identifies the absence of access by internal security authorities to VIS data as a short coming. The same could also be said for SISII[20] immigration and EURODAC[21] data.*[22]

The need for law enforcement to access this database for the fight against terrorism and security reasons has been generally accepted. VIS data in certain circumstances may become essential for law enforcement authorities. However, since the VIS is an information system developed for the application of border control, the general «routine access» of law enforcement may actually be a serious violation of the principle of purpose limitation. Most data subjects in the system are foreign travellers, who are required to hand in their biometric data for necessary examination before getting a visa. They are not actually expecting or informed about their data being used for other purposes (European Data Protection Supervisor 2006 b). The European Data Protection

18 VIS Regulation Article 8.
19 Id. Article 3.
20 The Schengen Information System (SIS), which became operational in March 1995, is a very important technological compensatory measure in the removal of internal borders in the Schengen cooperation and establishment of an area of freedom, security and justice. The SIS is a support tool both for free movement of persons and police cooperation. See further Karanja 2008.
21 Eurodac is originally a computerized database system for registering asylum seekers' fingerprint. Its scope has been extended through protocols to the Eurodac Convention (now Eurodac Regulations) to include registration of illegal immigrants' fingerprints.
22 COM (2005)597 final point 4.6

Supervisor commented on this change as a significant alteration of the system which could invalidate the results of the impact assessment study and the opinions of the data protection authorities. The EDPS stressed:

> *[o]ne must bear in mind that the VIS is an information system developed in view of the application of the European visa policy and not as a law enforcement tool … Access to the VIS by law enforcement can only be granted in specific circumstances, on a case by case basis and must be accompanied by strict safeguards» (European Data Protection Supervisor 2006 b).*

Information collected and retained by the US-VISIT will be accessed by employees of DHS components – i.e., Customs and Border Protection, Immigration and Customs Enforcement, Citizenship and Immigration Services, the Transportation Security Administration and by consular officers of the Department of State (Yonkers and Kelly 2003). *When necessary*, the information collected will be shared with other law enforcement agencies at the federal, state, local, foreign or tribal level, who are lawfully engaged in collecting law enforcement intelligence information and who need access to the information in order to *carry out their law enforcement duties* (Yonkers and Kelly 2003). According to the Privacy Impact Assessment (PIA) by the US-VISIT privacy officer, the collected data will be used for the purpose of border and immigration management, national security and law enforcement. Individuals have no opportunity to consent to or refuse the use of their data for these purposes, as this collection is mandated by law (Yonkers and Kelly 2003). The wording, such as «when necessary» and «law enforcement duties», seems to permit quite broad cross-sectoral applications, which would not appear to be in line with the use limitation principle in paragraph 10 of the OECD Privacy Guidelines to which the USA is at least politically committed to observing (OECD 1980). Compared with the strict limitation of access and use of the personal information in VIS, the privacy protection of the US-VISIT is quite weak, especially when considering most aliens' personal information will be excluded from the protection of the Privacy Act 1974. US-VISIT, as currently designed, will deny non-US citizens and residents the fundamental protection of the right to privacy.

All these facts indicate that the linking and tracking of biometric information are already happening in large-scale biometric systems for border control, and there are not adequate privacy safeguards for this function. Questions arise as to whether this indicates that the excessive linking and use of biometric information are already unstoppable? Could they be restricted in practice provided there were compelling reasons to do so?

3.4 Choice of technology and interoperability

Ann's passport is getting obviously thicker due to the different kinds of visas and biometric chips inserted in it. ICAO has recommended that, in the context of travel, facial recognition, fingerprint and iris scan appear to be the three primary candidates of choice for use as biometric identifiers in passports (Working Party on Information Security and Privacy 2004b). Each of them has different advantages and disadvantages. According to the principle of proportionality, biometrics should not include additional information, cannot be left anywhere easily and require the cooperation of the data subjects. However these criteria do not conclusively lead to one biometric feature (Hornung 2004, p. 50). Face recognition can be non-cooperative and fingerprints can leave traces on our everyday objects. Iris recognition avoids the main weakness of the above two; however, it discloses more additional information about the data subjects concerning health status, and it is less acceptable by people in general. On the whole each type of biometric bears its own advantages and disadvantages, but it is still possible that some country would like to choose to implement whichever biometric technology they see fit. If different countries use different technologies it will result in a thick passport as Ann encountered. The repeated collection of the same biometric identifier may also be caused by the non-interoperability of the biometric systems of different countries. It is possible that more and more countries will want to avoid costly enrolment procedures at local embassies by using the biometrics available on the passport. The promotion of e-passport schemes in Europe, using facial image and fingerprints, is a case in point.

The introduction of two biometric identifiers in European passports has raised a lot of concerns. It has been criticised as disproportionate to include the fingerprint in passports. In light of ECtHR case law, fingerprinting people is only justified particularly in the context of a prior criminal conviction or actual or potential prosecution against persons who have broken the law. There is nothing to suggest that fingerprinting everyone who holds a passport can be considered a justifiable interference with Article 8 rights under the ECHR. «The doubts about the proportionality principle are particularly cogent in light of the position of the US government and the ICAO standards related

to document security, which do not require fingerprinting for the purposes of travel document security» (Peers 2004).

However, the issue that raises more debate is the requirement of interoperability – i.e., «the ability of IT systems and of the business processes that they support to exchange data and to enable the sharing of information and knowledge» (Commission of the European Communities 2005). In Europe, there has been a great emphasis on facilitating interoperability and, thereby, data availability, particularly within the police and law enforcement sector (De Hert and Gutwirth 2006). Under the Prüm Treaty, for example, the police forces of EU Member States have had their ability to compare and exchange fingerprints, DNA samples and vehicle registrations enhanced.[23] The Commission has also issued a communication on interoperability and increased synergies between EU information systems, such as SIS, VIS and Eurodac, indicating gradual extension of the use of biometric technology in central EU information systems.[24] It has been claimed that biometric data will eventually become a primary key for storing and categorising all other forms of collected data (FIDIS 2006).

Once biometric and related data become accessible across national and organisational boundaries, the risk of such data being used for purposes other than the ones for which they were originally collected will persist if not increase (De Hert, P., W. Schreurs, et al. 2007, p.31). The enhanced interoperability of the biometric systems will serve to accentuate this risk. Critics of these developments oppose the use of biometrics as the primary data storage and connection key, as it would make the merging of different databases possible with very little effort, and enhanced key interoperability may bring about increased transparency of citizens, a development that is claimed to be «problematic in a democratic state keen on power-management» (FIDIS 2006) It will also increase the difficulties for data subjects in being able to monitor possibly illegitimate use and processing of their personal data. Another issue is the thorny question of who maintains authority over the data once they are transferred across organisational and/or national borders. The extensive movement of information whether to private companies or between public agencies, makes it very difficult to control the legitimate use of the data. The European Data

23 The Prüm Treaty was signed by the Contracting Parties in Prüm (Germany) on 27 May 2005, by Belgium, Germany, Spain, France, Luxembourg, The Netherlands and Austria. Significant parts of it (i.e., those parts dealing with police and judicial cooperation in criminal matters) were integrated into the EU legal framework in June 2007.

24 Cf. Commission Communication on improved effectiveness, enhanced interoperability and synergies among European databases in the area of Justice and Home Affairs, COM (2005)597 final (Brussels, 24.11.2005).

Protection Supervisor has expressed its concern about the enhanced interoperability between European databases and the creation of synergies between the mentioned systems, pointing out that:

> *Interoperability should never lead to a situation where an authority, not entitled to access or use certain data, can obtain this data via another information system» (European Data Protection Supervisor 2009, §24).*

At the same time, it is claimed that the push for greater interoperability has not taken sufficient account of the privacy-related concerns set out above. For example, the EDPS has commented: «It is regrettable that the protection of personal data has not been explored sufficiently as an inherent part of the improvement of the interoperability of relevant systems» (Best 2006).

The Biometric Storage System (BSS) in the USA will also facilitate biometric-based background checks by utilizing direct links to the FBI's IAFIS (Integrated Automated Fingerprint Identification System) network and US-VISIT/IDENT database. The BSS will facilitate biometrics-based identity verification. Once an applicant's biometric data are stored in the BSS, the identity can be authenticated through the US-VISIT/IDENT interface by comparing their fingerprint with the biometric (fingerprint) originally submitted to the BSS (US Department of Homeland Security 2006). There are also links between European databases and law enforcement agencies beyond Europe. Under the US-Europol agreement, signed in December 2001 and December 2002, personal data can now be exchanged between Europol and US law enforcement authorities.[25]

The interoperability between databases definitely increases the convenience of the biometric system but it also facilitates possible privacy invasions. This problem may be amplified when the interoperability is realised not only between databases within a country but between systems in different countries. It will become much easier to track people wherever they go. Although standardization seems to be the trend of future development, one needs to be aware that unless interoperability and privacy protection are achieved simultaneously, there is a direct trade-off between interoperability and the privacy protection *de facto* afforded by the non-interoperability.

25 See EU-US High Level Contact Group on Information Sharing and Privacy and Personal Data Protection (2008)

3.5 Central storage

Ann's biometric data are collected and stored in a central database. As mentioned previously, a key question about the privacy protection of biometric data is the place of data storage. Besides the security concerns of linkability and function creep, doubts attach to the value and effectiveness of such central storage. To what extent could the storage of biometric data of millions of innocent people in a central database help to prevent crime, when many terrorists do not need a visa to commit the crime?[26] There are two other main issues about central storage: (i) irreversibility, which concerns the likelihood that the subject of biometric data will not be able to revoke data and be victim to ID theft; (ii) connecting the personal data to another physical identity by only changing the biometric data and leaving the rest unchanged. While a counterfeit token requires only a copy to be made of the biometric template, accessing the central database will help obtain all the information needed. The potential economic value of such a huge biometric database may also pose a threat to people's privacy, as granting private institutions the rights to access these data may become a good way of making profit, which inevitably leads to function creep, and, arguably, breach of the proportionality principle (De Hert, Schreurs et al. 2007) The central database may also enable the police to search for a possible perpetrator of a crime with a presumption of all persons present in the database being suspects.

In cases where such central storage is chosen, like in the VIS and US-VISIT systems, protection measures are very essential. Essential among these are transparent procedures for access, use of the biometric data only by authorized authorities, a specified, finite retention period and a procedure for the data subjects to revoke their biometric data.

Both VIS and US-VISIT provide for publication of the list of the national authorities that are able to access the data in the centralized database.[27] Concerning the VIS, WP29 suggested that supplementary information on the authorized departments or offices and the access levels respectively assigned should be made available to data protection authorities in order for them to be in a better position to implement their supervisory duties (Article 29 Data Protection Working Party 2005 a). The VIS Regulation (Regulation 767/2008) envisages a period of 5 years for keeping the data (Article 23(1)); it also requires deletion of data on persons who have obtained the nationality of a Member State (Article 25). WP29 suggested this should also extend to perma-

26 For example as highlighted in the London bombings of July 2005, terrorists often live in the country where they intend to attack.

27 See VIS Regulation Article 6(3), and US Department of Homeland Security (2006) , p. 3.

nent residents of member states. WP29 also pointed out that a selective retention period is needed, for instance, it seems disproportionate to keep for more than 2 years data on visas issued for less than 3 months, especially where the short-term visit has concluded without particular incidents (Article 29 Data Protection Working Party 2005a).

In contrast, the US BSS will keep the biometric data for 75 years from the last recorded action. Besides the explanation of the purpose of the long retention period, the Privacy Impact Assessment of this system keeps silent about any kind of privacy risks this may raise. As noted above, aliens covered by the US-VISIT are generally not covered by the federal Privacy Act of 1974, and there are no additional regulations that deal with this issue as there are with the VIS. Unclear statements such as «for future use supports this initiative» from the Privacy Impact Assessment of the BSS, unavoidably raise much concern about the potential risks of the lengthy central storage of biometric information.

3.6 Security of RFID chips

In the scenario, Ann has to input a PIN-code before the machine starts reading the data stored in her passport; this is to secure the data stored there. The security and privacy threats posed by RFID tags which are used to store the biometric and other personal data in the MRTD, have raised much debate (EPIC 2005). RFID in itself is not a very secure technology. Tags can often easily be read using a reader and the wireless communication can be monitored by others

Under US-VISIT, all aliens are subject to biometric collection and watchlist checks. Use of RFID tags within the US-VISIT has been applied with privacy protection but has not been adequately configured and tested to ensure that those protections are effective, according to a report from the Homeland Security Department Inspector-General. Through these security lapses, someone could potentially swipe an unused RFID chip, program it into DHS's own database, and have a seemingly legitimate border-crossing document. It is found that while physical security controls over RFID systems have been adequate, computer security processes have been lacking which could allow unaut-

horized access or alteration of data in RFID system databases (Department of Homeland Security 2006). To deal with these threats, the Inspector-General recommended that the DHS should develop and implement policy and guidance that addresses security controls for systems being implemented using RFID technology, and ensure that this guidance be distributed into all the components, and is adhered to by all the security procedures (Department of Homeland Security 2006). In February 2007, the Department of Homeland Security announced that it had abandoned plans to use RFID technology in the US-VISIT border security system after pilot testing failed (House Homeland Security Committee 2007).

In November 2004, the Visa Working Group concluded that although the integration of the RFID chip safely storing the two biometric identifiers in the European passport would be technically possible, collisions between several RFID chips in a same document would make current plans to include visa stickers containing RFID chips into passports technically impossible (Visa Working Group 2004)[28]. The committee's report concluded that these plans should be dropped, and recommended that the visa sticker be accompanied by a separate smart card. This would solve the collision problem, as the card could be separated from the passport and read individually. An alternative would be to only store the biometric data in the VIS system (Visa Working Group 2004).

However, the EU and US Government had made decisions to begin issuing passports with embedded RFID tags to store the biometric data and other personal information. US-VISIT is also exploring the use of RFID technology as a tool that will better enable the program to fulfill its goals. The RFID tags are supposed to speed processing and increase security. According to the challenges to the policy issued by the Electronic Frontier Foundation (EFF)[29] and EPIC[30], identity thieves may break the encryption of the RFID tags and steal sensitive passport information using hand-held tag readers. The security problems surrounding RFID technology can be grouped in several classes:

1. data mining: the use of data-mining techniques to discover personal characteristics of an individual, which involve questions of privacy and data ownership issues;
2. data theft: given that RFID tags are made to broadcast information, it can be very easy for the concealable RFID scanners to steal this information.

28 By 01.02.2010 the author had not found further information on the progress of the combined RFID and biometric passport.

29 See generally EFF (2005)

30 See generally EPIC (2005)

However, security features are supposed to be added to the chips and data, such as secure encryption schemes.
3. Data corruption: when RFID tags, which are generally rewritable, are not locked (for example, in the supply chain), pranksters or malicious users will be able to re-write the tags with incorrect or fraudulent data.[31]

According to recent news reports, the security level of the current e-passport is still doubtful. In August 2006, a security consultant demonstrated at the Black Hat and Defcon security conferences in Las Vegas the method he used to crack an RFID-based e-passport like the one the US government planned to begin issuing to citizens. He also showed how he was able to clone the RFID chip inside the passport (Evers and McCullagh 2006).[32] Hence, the decision to implement this kind of data storage system raises a number of concerns regarding citizen privacy, as well as serious questions about the security of collected data.

3.7 Advanced risk analysis

In the scenario, Ann's personal data are automatically analysed in advance and she is allowed to use the green channel as a «low-risk» person, while some other people need to go through the blue channel or red channel. This scenario is designed based on the study of the Advanced Passenger Processing (APP) systems which allow for processing of API (Advanced Passenger Information) data before boarding or after take-off. Such systems process the information collected by the airline company during the check-in process. This information, called the passenger manifest, may be automatically collected from machine-readable travel documents (passports, visas or other documents). The information is electronically transmitted from the airline to the competent agency. The collected data are checked against lookout databases and may themselves feed other systems, for instance for tracking or profiling purposes (Working Party on Information Security and Privacy 2004a). For example, the Australian Department of Immigration and Citizenship is able to request an airline in a country outside Australia not to board an individual on a flight bound for Australia if the individual does not have a valid Australian visa or a valid Australian or New Zealand passport. At present, this program is called «iborders» and is developed by the SITA Corporation. The latter has supplied

31 Id.
32 The author has not found any later reports about the security improvement of the RFID chip in the passport.

the iborders system to authorities in Australia, New Zealand, Bahrain and Kuwait (SITA 2007).

Although neither the US-VISIT nor the VIS has adopted a similar advanced risk analysis program, it might be possible in the future. Many privacy risks are inherent in such a program, due to the storage, sharing, linking, tracking and profiling processes. Moreover, such kinds of automated decisions raise concern about how and to what extent people's rights should be determined on the basis of such a system. To what extent are and ought the biometric data represent the identity of a person in the computer world? How will individuals be affected by such representation? Another important question which has not yet been answered is whether biometrics can be revoked. If a person finds her biometric data have been compromised, and an automated decision is made on the basis of the compromised biometric data, maybe because the system finds an incorrectly allocated record of criminality, what can be done to revoke her biometrics and appeal the decision?

3.8 Usability, accuracy and quality of biometric systems

Facial recognition, as chosen by the ICAO, is also adopted in this scenario, and, as the scenario describes, such technology may raise several practical problems. These problems relate to its accuracy and usability, particularly in uncontrolled environments and with respect to users who are inexperienced or suffer from certain disabilities. Generally speaking, the usability of biometric systems will greatly influence their success and acceptance. The choice of biometric applications in different places needs to take into account the needs of the targeted group of people, in particular people with disabilities, elderly persons and children.

A person who fails a biometric test may either be an impostor or an honest person falsely rejected. Biometrics is influential in making the decisions of whether to grant an individual a visa, and whether to admit a traveller into a country. A key factor that must be considered is: if the biometric technology being used to perform a watch list check before visas are issued has a high rate of false matches, and the same biometric solution was used at the ports of entry, it could lead to increased delays in the inspection process. For security purposes it is important that fall back procedures are provided. The number of false rejections may be considerable in large-scale biometric systems. This may cause embarrassment and inconvenience to the individuals involved, and, accordingly, stresses the need for user-friendly secondary procedures.[33] Specific

33

concerns are with the quality of the biometric enrolment data: low quality biometric data will lead to a significant lower performance of the biometric matching system. Necessary procedures and considerations to compensate for this can affect the privacy of the data subjects.

To deal with these issues, Articles 37-39 of the VIS Regulation provide the data subjects the right to correct and delete inaccurate or unlawfully recorded data. A similar right is also given to individuals to inquire about the data US-VISIT has collected on them as well as to facilitate the amendment or correction of data that are not accurate, relevant, timely, or complete (DHS 2006a). However, tension exists between the actual implementation policies and the individual's right to participation. With the use of biometric information, it would be technically difficult for the individuals to know whether the biometric information on them is still accurate. What kinds of measures are available if there is physical damage to the data or the storage medium? The individual's participation right might become weak when biometric data are concerned. As emphasised by WP29, to guarantee effective fall-back procedures is of great significance as the biometric information «are neither accessible to all nor completely accurate» (Article 29 Data Protection Working Party 2005 a).

Instead of providing an alternative system at enrolment, the VIS exempts the category of people who are physically unable to be fingerprinted. Similarly, the US-VISIT may also provide exemptions to such groups of people at enrolment, though, as mentioned above, this is not clearly stated or determined by the regulations of the system.

In the EDPS's opinion on the SISII proposals,[34] comments are made on the level of accuracy of biometrics, noting in particular that the use of biometrics for identification is «more critical because the use of this process is less accurate» than authentication. Articles 18(5), 19(3) and 20(1)(2) of the VIS Regulation give the duly authorised staff the right to access data for further verification and identification where verification of the visa holder of the visa holder or of the visa fails. In the reports of the US General Accounting Office (GAO), it is only mentioned that when a «match» is found for the watch list from IDENT, the encounter data are stored as part of the US-VISIT process, and the traveller would be sent to secondary inspection for further action (GAO 2007).

34 Council doc 14091/05; OJ 2006 C 91

3.9 Health indication of biometrics

The concern that some biometric data may reveal racial origin or health status has been highlighted in the previous discussions. In this scenario, Ann is detected, through facial recognition technology, as possibly having some infectious disease. Generally speaking, biometric images (e.g., face, fingerprint, eye images, or voice signals) may show features that can reveal health information. In some cases, some of this information may remain in the template. It is quite possible that there can be medical systems that capture similar images to biometric systems, but use the information for diagnosis of disease and not for identification. Hence what needs to be considered is to what extent this kind of system should be allowed or prohibited? And if this is something that has to happen, how should it be restricted to a scope that does not unreasonably invade a person's privacy and dignity?

The preamble to the VIS Regulation (recital 12) states that any processing of VIS data «will be proportionate to the objectives pursued and necessary for the performance of the tasks of the competent authorities» and that «human dignity and integrity of the persons whose data is requested are respected». It has been emphasized that use of the data cannot lead to discrimination between visa applicants or visa holders on grounds of sex, racial or ethnic origin, religion, disability, age or sexual orientation (Justice and Home Affairs 2007). Socialist MEP Fausto Correia, who presented a report on data sharing between police forces, said: «The inclusion of the Prüm Treaty in EU law, and its extension, must preserve the confidentiality of personal data. Information about ethnic origins, sexual orientation or health should be dealt with only in cases of absolute necessity» (Euractive 2007). There are, however, no actual provisions that address the possible disclosure of health information by the biometric information in the VIS Regulation.

In the fact sheet issued by the US Department of Homeland Security, it is emphasized that US-VISIT will assure that the visitors' information is always protected. Yet there is no discussion about potential use of biometric information to track visitors' health status. It can be safely concluded at present that this issue has not been seriously addressed by either of the two legal regimes.

4 Conclusions

This paper has described and discussed various possible legal concerns that may emerge at a biometric border-control system. The detailed comparison and description of the different policy and legal regulations of the VIS and US-VISIT systems show that the current regulations of biometrics in this context are inadequate to protect individuals' privacy rights. Some legal or policy

proposals have emerged in Europe, while the protection of privacy has not got enough attention in the US scheme, especially concerning the US-VISIT system. One important reason might be that it is a system concerning *aliens'* travel to the USA.

The technical characteristics and limitations of biometric systems should be used as the basis for legal regulation of such systems. Quality concern limitations, health indications and the security concerns of RFID are problems that directly link to the development of biometric techniques. Interoperability and access limitation, age exemptions, adoption of central databases, and advanced risk analysis are more concerned with how the system is used. However, these two sides are closely connected. The development of the biometric technology will definitely influence the way of using biometrics and its risk to privacy. Hence, the corresponding regulations should take into account the future development of the technology.

Bibliography

Article 29 Data Protection Working Party (2005a). Opinion 2/2005 on the Proposal for a Regulation of European Parliament and of the Council concerning the Visa Information System(VIS) and the exchange of data between Member States on short stay-visas, COM(2004) 835 final 1022/05/EN WP110

Article 29 Data Protection Working Party (2005 b). «Opinion 3/2005 on Implementing the Council Regulation (EC) No 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States.» Retrieved 15.02.2010, from http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp112_en.pdf.

Best, J. (2006). «Biometrics unreliable, says EU privacy head, CNET News.com.» Retrieved 15.02.2010, from http://www.news.com/Biometrics-unreliable,-says-EU-privacy-head/2100-1029_3-6050024.html.

Commission of the European Communities (2005). Communication to the Council and the European Parliament on improved effectiveness, enhanced operability and synergies among European Parliament on improved effectives, enhanced operability and synergies among European Databases in the area of Justice and Home Affairs, COM (2005) 597 final,25 November 2005, Brussels, Belgium.

De Hert and Gutwirth (2006). «final op cit Interoperability of police databases within the EU: an accountable political choice.» *International Review of Law, Computers and Technology* Vol. 20: 22 - 35.

De Hert, P., W. Schreurs, et al. (2007). «Machine-readable identity documents with biometric data in the EU - part IV, critical observations.» *Keesing Journal of Documents & Identity.* Vol. 24: 29 -35.

Department of Homeland Security (2004). «Notice to Aliens Included in the United States Visitor and Immigrant Status Indicator Technology (US-VISIT) Program.» Retrieved 15.02.2010, from http://edocket.access.gpo.gov/2009/E9-12939.htm.

Department of Homeland Security (2006). «Privacy Impact Assessment Update for the United States Visitor and Immigrant Status Indicator Technology (US-VISIT) Program.» Retrieved 16.02.2010, from http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_usvisit_addaliens.pdf

Department of Home Land Security (2009) US-VISIT Enrolment Requirements, last visited 4 February 2010 at http://www.dhs.gov/files/programs/editorial_0527.shtm

EFF (2005). «EFF's proposal to Chief, Legal Division Office of Passport Policy, Planning and Advisory Services, dated April 4, 2005.» Retrieved 15.02.2010, from http://www.eff.org/files/filenode/rfid/RFID_passport.pdf.

EPIC (2005). «Comments of the Electronic Privacy Information Center.» Retrieved 15.02.2010, from http://www.epic.org/privacy/us-visit/comments080405.html

European Data Protection Supervisor (2006 a). «Opinion of the European Data Protection Supervisor on the Proposal for a Regulation of the European Parliament and the Council amending the Common Consular Instructions on visas for diplomatic missions and consular posts in relation to the introduction of biometrics including provisions on the organisation of the reception and processing of visa applications (COM (2006) 269 final) —2006/0088 (COD) (2006/C 321/14) «. Retrieved 15.02.2010, from http://www.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2006/06-10-27_CCI_EN.pdf.

European Data Protection Supervisor (2006 b). «Opinion of 20 January 2006 on the proposal for a Council Decision concerning access for consutation of the Visa Information System(VIS) by the authorities of Member States responsible for internal security and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences (COM (2005) 600 final).» Retrieved 15.02.2010, from http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2006/06-01-20_Access_VIS_EN.pdf.

European Data Protection Supervisor (2009). «Data protection legislation.» Retrieved 15.02.2010, from http://www.edps.europa.eu/EDPSWEB/edps/Home/EDPS/Dataprotection/Legislation.

Evers, J. and D. McCullagh (2006). «E-passports pose security risk, from ZENT news Aug 5 2006.» Retrieved 15.02.2010, from http://www.news.com/Researchers-E-passports-pose-security-risk/2100-7349_3-6102608.html.

FIDIS (2006). «Future of identity in the information society.» Retrieved15.02.2010, from http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp6-del6.1.forensic_implications_of_identity_management_systems.pdf.

GAO (2007). «Information Security Homeland Security Needs to Immediately Address Significant Weaknesses in Systems Supporting the US-VISIT Program.» Retrieved 15.02.2010, from http://www.gao.gov/new.items/d07870.pdf

Hornung, G. (2004). Biometric identity cards: Technical legal and policy issues. *Securing Electronic Business Processes*. S. Paulus, N. Pohlmann and H. Reimer. Germany, Friedrick Vieweg & Son Vol.: 47 -- 57.

House Homeland Security Committee (2007). «REP. Bennie Thompson holds a hearing on the FISCAL year 2008 Department of Homeland Security Budget.» Retrieved 16.02.2010, from http://www.epic.org/privacy/us-visit/chertoff_020907.pdf

Kingsbury, N. (2002). «Technology Assessment: Using Biometrics for Border Security. United States General Accounting Office (USGAO), report# GAO-03-174, Nov.»Retrieved 16.02.2010, from http://www.gao.gov/new.items/d03546t.pdf.

OECD (1980). *Guidelines Governing the Protection of Privacy and Trans-Border Flow of Personal Data, OECD Doc.58 final (Sept.23 1980) art.3 (a)*, Privacy Law Sourcebook.

Peers, S. (2004). «The Legality of the Regulation on EU Citizens' Passports», 26 November 2004, pp.1-4. Retrieved 16.02.2010, from http://www.statewatch.org/news/2004/nov/legal-analy-bio-passports.pdf.

Seghetti, L. M., & Viña, S. R. (2005). «U.S. Visitor and Immigrant Status Indicator Technology (US-VISIT) Program», CRS report for congress. Retrieved Nov.1, 2007, from http://www.fas.org/sgp/crs/homesec/RL32234.pdf

SITA (2007). «iBorders.» Retrieved 16.02.2010, from http://www.sita.aero/Solutions/Border_management_solutions/iBorders.htm.

Yonkers, S. and N. O. C. Kelly (2003). «US-VISIT Program, Increment 1 Privacy Impact Assessment Executive Summary, Department of Homeland Security «. Retrieved 16.02.2010, from http://www.privacyinternational.org/issues/terrorism/library/USVISITPIAfinalexecsum1_.pdf

Visa Working Group (2004). «Integration of aspects of biometric identifiers in the uniform visa format and in the uniform residence permit for third country-nationals, Council of European.» Retrieved 16.02.2010, from http://www.statewatch.org/news/2005/jan/bio-visas-16257.pdf.

Working Party on Information Security and Privacy (2004 a). «Background Material on Biometrics and Enhanced Network Systems for the Security of International Travel DSTI/ICCP/REG (2003)3/FINAL.» Retrieved 16.02.2010 from http://www.oecd.org/dataoecd/16/18/34661198.pdf

Working Party on Information Security and Privacy (2004 b). «Biometric-based technologies.» Retrieved 16.02.2010, from http://www.cnipa.gov.it/site/_files/DSTI-ICCP-REG-(2003)2-REV2.pdf

DEN MENNESKELIGE FAKTOR I ELEKTRONISK FORVALTNING[1]

Dag Wiese Schartum

1 Innledning

Forvaltningen i de nordiske landene gjør i stigende grad bruk av IKT. [2] Teknologiens massive inntog i forvaltningsorganene har konsekvenser for hvorledes forvaltningen utfører sitt arbeid. Ikke minst kan den virke inn på forholdet mellom de ansatte i forvaltningsorganet og borgerne som henvender seg til forvaltningen. Peter Blume har i stor grad vært opptatt av enkeltindividets situasjon i informasjonssamfunnet, og særlig spørsmål vedrørende persondatabeskyttelse. I denne artikkelen tar jeg opp enkelte spørsmål vedrørende borgernes kontakt med forvaltningen når saksbehandlingen er digitalisert. Bakgrunnen er en spørreundersøkelse fra april 2009 om holdninger blant ansatte i norsk offentlig forvaltning til at opplysninger om dem blir gjort tilgjengelig på Internett. Spørsmålene kan vurderes ut i fra hensynet til persondatabeskyttelse (eller «personvern»), men kan også ses i lys av rettssikkerhet, offentlighet og effektivitet.

2 Elektronisk forvaltning

Elektronisk forvaltning (eForvaltning)[3] er i litteraturen definert på flere ulike måter. Begrepet kan brukes for å betegne aktiviteter. Elektronisk journalføring kan for eksempel ses på som en elektronisk forvaltningsaktivitet. Alternativt kan vi bruke begrepet mer overordnet, som en samlende beskrivelse av kjennetegn ved noen forvaltningsorganisasjoner. Uansett vil de fleste trolig være enige i at det ikke gir særlig mening i å bruke eForvaltning bare fordi et forvaltningsorgan bruker datamaskiner på «selvfølgelige måter» (tekstbehandling, epost mv). Poenget med et slikt begrep må jo være å formidle at elektronisk forvaltning arbeider på andre måter enn forvaltningen for øvrig. Begrepet

---

1 Artikkelen er opprinnelig publisert i Ret, informatik, samfund: festskrift til Peter Blume.- København, 2010.

2 Dvs. hjelpemidler som gjør bruk av informasjons- og kommunikasjonsteknologi.

3 Eller «digital forvaltning», engelsk: «eGovernment».

vil dessuten bli uinteressant dersom *all* forvaltning kan sies å være elektronisk. For at begrepet eForvaltning skal være til nytte, kan det derfor hevdes en forutsetning om at det må foregå en eller annen kvalifisert form for bruk av elektroniske hjelpemidler. Én mulighet er å stille opp kriterier om hvor vesentlig innslaget av elektronisk behandling skal være. Utgangspunktet kan være en klassifisering av det utstyret forvaltningen gjør bruk av. Vi kan for eksempel legge vekt på graden av automatisert utøvelse av myndighet og tjenesteproduksjon, graden av elektronisk kommunikasjon mv.

Enkelte definisjoner legger vekt på *formålet* med forvaltningens bruk av IKT og forventede effekter. Slik er det for eksempel i dokumenter fra EU-kommisjonen:

> *«eGovernment is defined here as the use of ICT in public administration combined with organisation changes and new skills* ***in order to improve public services*** *and democratic processes and strengthen support to public policies.» (min utheving)*[4]

En noe snevrere og mer spesifikk definisjon kan vi finne i USAs Electronic Government Act:

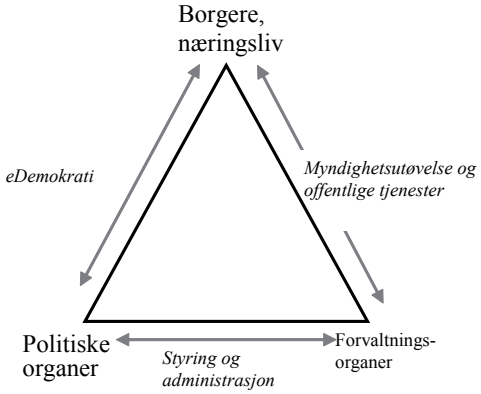
> *«The use by the government of Web-based Internet applications and other ICTs, combined with processes that implement these technologies,* ***to a) enhance the access to and delivery of government information and services to the public****, other agencies, and to government entities; or bring about improvements in government to operations that may include effectiveness, efficiencies, service quality, or transformation.» (min utheving)* [5]

I figur 1 forsøker jeg å gi et samlet bilde av eGovernment. Her inngår bl.a. eDemokrati som primært gjelder forholdet mellom politiske organer og det sivile samfunn. eForvaltning kan sies å gjelde *alle øvrige* deler av forvaltningens oppgaveløsning, dvs. forvaltningens egenforvaltning (material-, personal- og økonomiforvaltning mv), myndighetsutøvelse (enkeltvedtak, forskrift, politiske vedtak, planarbeid, mm), samt ulike former for offentlig tjenesteyting (ut-

4 COM (2003) *The Role of eGovernment for Europe's Future*. Communication from the Commission to the Council COM (2003) 567 Final, avsnitt 3. Brussels 26.9.2003, se http://ec.europa.eu/information_society/eeurope/2005/doc/all_about/egov_communication_en.pdf.

5 US government (2002) The e-government act of 2002. HR 2458, "§ 3601. Definitions (3), se http://csrc.nist.gov/drivers/documents/HR2458-final.pdf.

danning, helse, samferdsel, kultur osv).[6] Her er det ikke grunn til å gå nærmere inn på de mange enkeltspørsmål som kan reises i forbindelse med hva som er etablert og hensiktsmessig begrepsbruk knyttet til elektronisk forvaltning. Poenget her er primært å lokalisere den høyre siden av trekanten der borger og forvaltningsorgan møtes med IKT som hjelpemiddel.



Figur 1: Illustrasjon av hovedelementer i «eGovernment»

I begge sitatene ovenfor har jeg kursivert elementer som uttrykker målsettinger om å forbedre informasjon og tjenester overfor borgere. Stort sett presenteres gjerne elektronisk forvaltning som tjenesteleverandør (jf «services»), men innenfor rammene av denne artikkelen er bruk av IKT i forbindelse med offentlig *myndighetsutøvelse* av størst betydning. I fortsettelsen legger jeg således primært vekt på forvaltningens bruk av IKT i tilknytning til vedtak som etablerer plikter og rettigheter i enkeltsaker.

Målsettingene om å forbedre oppgaveløsningen i forvaltningen, herunder forbedre myndighetsutøvelsen ved hjelp av IKT, minner oss om at forandring og forbedring forutsetter en kvalitetsnorm. Som den andre definisjonen ovenfor viser, kan effektivisering, bedre tjenestetilbud og omstillingsdyktighet være blant de kvaliteter en velger å etterspørre. Hadde jurister spesifisert kvalitetsmålene ville dessuten bedret rettssikkerhet, ivaretakelse av personvern, samt bedre realisering av offentlighetsprinsippet trolig vært blant disse.

6 I tillegg anvendes IKT selvfølgelig også innen den politiske og intern administrative styringen av forvaltningen, og denne forholder seg både til demokrati- og forvaltningssiden av trekanten i figur 1.

I politiske dokumenter vedrørende elektronisk forvaltning kan det hevdes å være en tendens til at alle gode formål formuleres som målsettinger samtidig, uten at forholdet mellom dem klargjøres nærmere. Det må imidlertid erkjennes at det kan være et motsetningsforhold mellom ønske om effektivitetsforbedringer og kostnadsreduksjoner på den ene side, og ivaretakelse av den enkeltes rettigheter og integritet på den annen side. Garantier for rettssikkerhet og personvern og realisering av offentlighetsprinsippet, kan åpenbart medføre arbeidsbelastning og kostnader, og effektiviseringstiltak kan tenkes å svekke borgernes beskyttelse og rettigheter. Det er imidlertid neppe noen automatikk i slike negative følger for borgerne. Dersom en søker å forene ulike hensyn, kan eForvaltning både gi effektivitetsgevinster og bedre beskyttelse for enkeltindividet mv. Et saksbehandlingssystem kan for eksempel både gjøre det mulig å redusere ressursinnsatsen og samtidig gjøre saksbehandlingen grundigere, fordi beslutningsgrunnlaget kan gjøres mer tilgjengelig, fullstendig og korrekt i et elektronisk system enn med en manuell arbeidsmåte.

Det er heller ikke nødvendigvis full harmoni i forholdet mellom ulike interesser som borgere kan sies å ha. Ethvert rettssikkerhetstiltak er for eksempel ikke uproblematisk for personvernet: Rett til partsinnsyn kan gi motparten tilgang til personopplysninger som den andre parten ønsker å beskytte. Skjerming av personopplysninger kan også tenkes å svekke forvaltningens beslutningsgrunnlag og dermed sette rettssikkerheten i fare. Selv om personvern langt på vei begrunner åpenhet,[7] kan personvern bidra til å begrense allmennhetens og parters rett til innsyn. IKT som brukes for å effektivisere en type ideell interesse, kan med andre ord tenkes å ville skape eller skjerpe konflikter mellom ulike beskyttelser og rettigheter som er gitt den enkelte borger.

Disse enkle erkjennelsene er bakteppet for den følgende framstilling som tar utgangspunkt i hovedresultater fra en undersøkelse av i hvilken grad og på hvilken måte forvaltningsorganer i Norge eksponerer sine ansatte på nettet.

3 Offentlig ansatte på nett

Elektronisk forvaltning i Norden er i stor grad bygget på selvbetjening og automatisering. Med selvbetjening sikter jeg for det første til forventningen om at borgerne skal sette seg inn i, forstå og innrette seg etter den informasjon som forvaltningen gjør tilgjengelig på sine nettsider. For det andre sikter jeg til beslutningsprosesser der den enkelte part selv «er sin egen saksbehandler» ved å inngi opplysninger i forvaltningsorganets informasjonssystem på net-

7 Se lov om behandling av personopplysninger mv av 14. April 2000 nr 31, § 18 første ledd, jf den danske Persondatalov av 31. Mai 2000 nr 429, § 54 Stk 1.

tet, for dermed å igangsette en helt eller delvis automatisert saksbehandling. Automatisering innebærer bl.a. at rettsreglene gis en representasjon i datamaskinprogrammer, slik at rettsanvendelsen lar seg automatisere. Høy automatiseringsgrad er noe som særpreger offentlig forvaltning i Norden, og særlig innen forvaltningsområder der det skjer fordeling og omfordeling av penger i samfunnet[8] er graden av automatisering høy. Også innen opptak til skoler og universiteter finnes det rutiner som i meget stor grad baserer seg på automatiske rutiner. I Norge, Danmark og andre vestlige land er automatiseringsgraden trolig økende, og på enkelte forvaltningsområder er saksbehandlingen nesten fullstendig automatisert.[9]

Elektronisk forvaltning kan sies å ha et potensial for å virke fremmedgjørende, dvs. IKT-bruk i forvaltningen kan skape situasjoner med usikkerhet og frustrasjon. Selv om informasjonssystemene grunnleggende sett er rasjonelt laget og godt brukbare for flertallet av borgerne, vil enkelte kunne ha problemer med å forstå hvorledes systemene skal anvendes, hvilken sammenheng de opptrer i mv. Også for personer som har erfaring med teknologi kan kompliserte og lite transparente elektroniske saksbehandlingsrutiner skape følelse av usikkerhet og maktesløshet. I slike situasjoner kan vi ha behov for å kommunisere direkte med en saksbehandler i forvaltningsorganet.

Et fellestrekk ved selvbetjening og automatisering, er at den enkelte borger ikke trenger, og ikke forutsettes å ha kontakt med en saksbehandler. Det vi tilbys er i meget stor grad standardisert informasjon og tilrettelegging. Våre individuelle behov og preferanser kan bare i begrenset grad imøtekommes innenfor rammene av denne form for elektronisk forvaltning. Likevel er det standardiserte tilbudet tilstrekkelig og ofte godt nok i kurante saker, og det er tross alt de vanlige sakene som dominerer bildet. Dersom saken vår er *ukurant*, dvs. dersom informasjonen og rutinene vi tilbys på nettet ikke passer med våre særlige, individuelle behov, kan vi imidlertid ha ønsker om å snakke med noen for å få konkret hjelp.

Uansett om vi er blant de fremmedgjorte eller blant de veltilpassede brukere med ukurante saker, har vi med andre ord behov for noen å kommunisere direkte med, dvs. ringe eller sende epost til, eller til og med avtale møte med. Det er derfor vel begrunnet å legge til rette for at borgerne skal kunne ta kontakt med saksbehandlere som har kunnskaper og fullmakter til å hjelpe oss dersom teknologien er uforståelig eller svikter. I stedet for – som tidligere – å måtte spørre oss fram på et sentralbord og høre på dårlig musikk mens vi venter på

8 For eksempel skatt, pensjoner, støtte- og tilskuddordninger mv.

9 Et sentralt forvaltningsområde med veldig høy grad av automatisering er ligning av personlige skattytere.

svar, kan forvaltningens nettsider sette oss i stand til å ta direkte kontakt med saksbehandler på epost, mobil mv. [10] I hvilken grad benyttes slike muligheter?

I mars 2009 gjennomførte jeg en spørreundersøkelse som tok sikte på å kartlegge i hvilken grad norsk forvaltning eksponerer sine ansatte på nettet ved å gjøre tilgjengelig kontaktopplysninger, personbilde mv.[11] Til grunn for undersøkelsen lå kunnskapen om at personopplysningsloven[12] setter grenser for forvaltningens[13] mulighet til å pålegge at opplysninger om den enkelte arbeidstaker er tilgjengelig på slike måter. Samtidig tilsier ofte åpenhet i forvaltningen og høyt servicenivå at slik informasjon finnes. Hensynet til de ansattes personvern kan tale i mot at opplysninger om dem blir eksponert på nettet. Personvern er imidlertid ikke eneste hensyn som kan trekke i restriktiv retning. En kan for eksempel anta at allmenn tilgang til kontaktopplysninger om saksbehandlere vil gi flere avbrytelser i arbeidet og dermed mindre effektiv utnyttelse av arbeidstiden - noe som i sin tur kan gi lengre saksbehandlingstider. Ikke minst kan det være fare for at epost direkte til den enkelte (og ikke via sentrale postmottak) gir fare for at henvendelser det er plikt til å journalføre ikke blir registrert. Sviktende journalføring vil kunne gi redusert realisering av offentlighetsprinsippet og svekkelse av muligheter for innsyn fra andre. Selv om hensynene for å gjøre kontaktopplysninger mv tilgjengelig på forvaltningens nettsider er sterke, er det med andre ord ikke opplagt at de er tilstrekkelig sterke til å slå igjennom. Uansett foreligger det etter norsk lov stor grad av valgfrihet i spørsmålet, og det er derfor interessant å legge merke til hvilke valg ulike deler av forvaltningen har gjort.

Første del av opplegget gikk ut på å kartlegge hvor vanlig det er at kontaktopplysninger til ansatte er gjort tilgjengelig på forvaltningens nettsider. Utgangspunktet var her et utvalg på i alt 89 kommuner og 15 statlige direktorater og tilsyn. Denne delen av undersøkelsen gikk ut på manuell gjennomgang av alle de aktuelle nettsidene. Resultatet viste at 38 kommuner (42,7 %) og 10 statsetater (66 %) hadde gjort epostadresser og andre personlige opplysninger om sine ansatte tilgjengelige fra organisasjonens nettside.[14]

---

10 Det må understrekes at slik teknologibruk ikke hjelper den som over hodet ikke kan bruke IKT, for eksempel store grupper av den eldste befolkningen. Indirekte kan imidlertid også de oppnå forbedringer fordi det vil være enklere for andre (familien, venner, naboer mv) å hjelpe dem.

11 Takk til masterstudent Ivar Berg-Jacobsen og bachelorstudent Jorid Heggelund som utførte innledende analyse av nettstedene og grovsortering av de innkomne resultatene fra selve spørreundersøkelsen.

12 Lov av 14. april 2000 nr 31, her forkortet «pol».

13 Som «behandlingsansvarlig» og arbeidsgiver, jf pol § 2 nr 4, jf «dataansvarlig» i den danske Persondatalov av 31. Mai 2000 nr 429, § 3 nr 4.

14 Svarprosenten var markert høyere i staten (27 %) enn i kommunene (10 %).

En epost med lenke til et spørreskjema ble sendt til i alt 1014 ansatte som hadde tilgjengelige epostadresser på arbeidsstedets nettsider. Av disse svarte 151 personer, eller 13,5 %. Svarene belyser bl.a. i hvilken grad slike kontaktopplysninger kan oppfattes som et problem for de ansattes personvern, men vi hadde også med spørsmål om hvorledes direkte henvendelser til ansatte ble håndtert i forhold til journalføring mv.

Publisering av opplysninger om ansatte kan som nevnt skje på grunnlag av samtykke fra den enkelte. For at forvaltningen som arbeidsgiver skal kunne *pålegge* sine ansatte å legge ut opplysninger om dem på nettet, må de i praksis kunne vise til en «nødvendig grunn», slik disse er regnet opp i pol § 8.[15] Mer konkret er alternativene i bokstav a (nødvendig for å oppfylle en avtale med den registrerte) og bokstav e (nødvendig for å utøve offentlig myndighet) spesielt aktuelle. Det kan også være aktuelt å vise til § 8 bokstav f som gir anvisning på en bred interesseavveining mellom hensynet til personvern og motstående berettigede interesser. På bakgrunn av avgjørelse i Personvernnemnda er det imidlertid neppe mulig å legge dette alternativet til grunn med mindre det foreligger tilstrekkelige grunner til ikke å basere seg på samtykke fra de registrerte.[16] Her kommer jeg ikke nærmere inn på mulige rettslige grunnlag for at forvaltningen skal kunne legge ut opplysninger om sine ansatte på nettet. Hovedpoenget er at den enkelte persons selvbestemmelse står sterkt, noe som gjør samtykke til det primære og mest aktuelle rettslige grunnlaget. Også «nødvendige grunner» som nevnt, kan imidlertid tenkes å være grunnlag.

I spørreundersøkelsen stilte vi spørsmål som er egnet til å belyse om kravene i pol § 8 etterleves eller ikke. I en undersøkelse med respondenter som ikke kan forventes å kjenne lovgivningen og dens begreper i detalj, er det ikke tjenlig å formulere spørsmål som direkte samsvarer med lovens systematikk og ordlyd. En kan heller ikke forutsette at lovens system har vært bestemmende for vurderingen av spørsmålet. Vi stilte derfor spørsmål om hva som var det viktigste grunnlaget for å legge ut opplysninger om ansatte på nettet, og oppgave alternativene: «Fast ordning», «nødvendig», «arbeidsavtalen», «samtykke» og «vet ikke». Svarene vi fikk tyder på at nevnte lovregulering har liten effekt på spørsmålet om rettslig grunnlag for publisering av opplysninger om ansatte (se tabellen).

15 Alternativt kunne det ha vært vis til hjemmel i lov, men slik lovgrunnlag finnes ikke.
16 Se Personvernnemndas vedtak i klagesak 2004/1, tilgjengelig fra Personvernnemnda.no.

Fast ordning	53,7 %
Nødvendig	25,8 %
Arbeidsavtalen	5,3 %
Samtykke	5,3 %
Vet ikke	9,9 %
	100,0 %

Svaralternativet «fast ordning» viser ikke til noe rettslig kriterium. Sammenholdt med alternativet «nødvendig», kan svaret «fast ordning» imidlertid leses som uttrykk for at spørsmålet er utenfor diskusjon, dvs. at ordningen er fast etablert. «Nødvendig» gir mer uttrykk for at ordningen med å legge ut opplysninger om ansatte på nettet har en kjent begrunnelse, men gir ikke signal om det er gjennomført en rettslig vurdering av kravene i pol § 8 og de «nødvendige grunner» som er angitt der. Svarene gir klart bilde av at utlegging av opplysninger om ansatte på nettet ofte er en fast praksis som de ansatte selv har liten innflytelse på. Selv om en ikke kan utelukke at ansatte har hatt innflytelse i de 79,5 % av svarene der slik publisering er angitt som fast ordning eller nødvendig, er det kun i de 10,6 % av svarene av kategoriene «arbeidsavtalen» og «samtykke» at det direkte er rom for medbestemmelse for den enkelte.

Tallene sier ingen ting sikkert om praksis er styrt av gjeldende regler i pol § 8. Svar om at det gjelder en fast ordning, kan muligvis romme tilfelle der ordningen i sin tid har vært vurdert som nødvendig etter § 8 bokstavene a – f, men senere ikke har vært til diskusjon. Svar om at ordningen er «nødvendig» kan likeledes peke til «nødvendig grunn i § 8, men kan også kun referere til respondentens uavhengige oppfatning. På den annen side ser det ut til å være en sikker konklusjon at samtykke på dette området spiller en ytterst beskjeden rolle (5,3 %). Sett på bakgrunn av den norske Personvernnemndas standpunkt om at samtykke er hovedregel i relasjon til kriteriet nødvendig grunn i pol § 8, er dette et interessant resultat. Overfor egne ansatte vil det nettopp være enkelt å innhente samtykke. Det kan heller ikke antas å skape særlige problemer dersom ansatte (delvis) motsatte seg å bli eksponert på forvaltningens nettsider.

På direkte spørsmål om ordningen med publisering av opplysninger om dem var frivillig eller ikke, svarte 44,4 % at det ikke var frivillig, mens 25,8 % angav at det dreiet seg om en delvis frivillig ordning (for eksempel slik at en kan motsette seg personbilde mv). Kun 13,9 % angav ordningen som helt frivillig. Tallene bekrefter inntrykket av at praksis er basert på arbeidsgivers ensidige vurdering som gir liten anledning til medbestemmelse for den enkelte.

Vi spurte også om hva slags opplysninger som lagt ut om ansatte. I de aller fleste tilfellene var det grunnleggende opplysninger som navn, stilling/oppgaver

og kontaktinformasjon vedrørende arbeidsstedet som var gjort tilgjengelig. Et relativt lite antall av respondentene (28) angav også at det ble publisert personbilde. I noen få tilfelle ble det også angitt opplysninger av rent privat karakter.

På spørsmål om hvor godt begrunnet respondentene mente praksis med publisering av opplysningene var, svarte hele 80,8 % at alle/de fleste opplysninger var vel begrunnet. Kun 5,3 % mente at ingen av de aktuelle opplysningene var godt begrunnet å publisere på nettet. Et markert flertall av respondentene (86,7 %) hadde aldri hatt ubehag på grunn av at opplysninger om dem var tilgjengelig på nettet, og ingen var ofte plaget.[17] Flere av merknadene som ble gitt i spørreskjemaets fritekstfelt gav imidlertid uttrykk for motstand mot publisering av personbilde.

På en måte er tallene fra denne delen av undersøkelsen lite dramatiske: Forvaltningen legger kun få og grunnleggende opplysninger om sine ansatte ut på nettet, og langt de fleste synes dette er vel begrunnet og har ikke negative erfaringer med ordningen. På den annen side kan det se ut som om praksis er etablert uten at de sentrale lovbestemmelser som regulerer spørsmålet er tatt hensyn til. Dette fører til at graden av medbestemmelse og frivillighet er lav. De ansattes gjennomgående positive/ikke negative holdning til at opplysninger om dem blir publisert, skulle nettopp legge til rette for å tillegge ansattes meninger stor vekt. Dersom arbeidsgiver har inntrykk av stor grad av aksept blant ansatte, vil imidlertid dette kunne brukes som begrunnelse for å la være å spørre: Dersom en skal sette i gang et stort arbeid med å innhente samtykke, bare for å bekrefte «det alle vet», at ordningen er akseptabel for de aller fleste, kan dette oppfattes som anstaltmakeri. Etter loven vil det imidlertid være en feilslutning å tenke på spørsmålet om aksept som et spørsmål om hva flertallet av de ansatte vil. Samtykke skal legge til rette for individuelle valg, og har ikke minst sin berettigelse i situasjoner der noen få personer ikke ønsker å bli eksponert på grunn av individuelle omstendigheter. En kvinnelig ansatt som lever i frykt for sin tidligere ektemann, en ansatt som behandler saker med høyt konfliktnivå, og en ansatt med fobier, vil for eksempel kunne ha gode grunner for å unngå eksponering av egen person på nettet som bør respekteres. Fravær av opplysninger om seg selv på nettet gir selvsagt ingen anonymitet, men kan gi større grad av fred og skjerming i forhold til omverdenen. Selv om det kan dreie seg om få personer – eller kanskje nettopp derfor – er det grunn til å legge til rette for og respektere ansattes individuelle valg. Dermed er det ikke sagt at publisering av opplysninger om ansatte nødvendigvis bør baseres på samtykke slik hovedregelen etter norsk rett er i dag. Rettspolitisk sett kan

17 11,3 % var plaget av og til.

alternativet for eksempel være en ordning med *kollektivt* samtykke[18] kombinert med en rett for den enkelte til å velge å stå utenfor ordningen («opt out»).

4 Elektronisk forvaltning med menneskelig ansikt

I norsk personvernteori har det i over 30 år vært vanlig å hevde at folk typisk har en interesse i en «brukervennlig behandling».[19] Interessen har bl.a. vært forklart med et krav om uhindret dialog, dvs. at det i minst mulig grad skal være formelle og praktiske hindre som står i veien for kontakt mellom de registrerte og den behandlingsansvarlige.[20] Interessen innebærer at det ses som positivt for personvernet at den enkelte borger lett kan komme i kontakt med saksbehandlere og andre personer i forvaltningen som kan gi svar på spørsmål vedrørende behandling av personopplysninger om dem. Det kan dermed oppstå et spenningsforhold mellom denne interessen og enkelte ansattes ønske om og ikke bli (for meget) eksponert på forvaltningens nettsider. Ansattes personvern kan stå delvis i motsetning til borgeres interesse i å finne fram til den rette person å snakke med. Den refererte undersøkelsen vedrørende utlegging av opplysninger om ansatte på nettet, kan imidlertid tyde på at dette i liten grad er en reell problemstilling. Dersom en liten andel ansatte ønsker å reservere seg mot å bli eksponert på nettet, vil heller ikke det gjøre det nevneverdig vanskeligere å formidle kontakt mv til saksbehandlere. Derfor er det neppe hensynet til de ansattes personvern som er det viktigste argumentet mot å publisere opplysninger om ansatte og dermed øke muligheten for direkte kontakt med et menneske. Kun 34 av 89 kommuner og 4 av 15 statsetater i undersøkelsen gav tilgang til *alle* sine ansattes epostadresser.[21] Årsaken til at flertallet av forvaltningsorganene har valgt ikke å gi tilgang til epostadresser mv, er trolig å finne i andre hensyn enn personvern. Her vil jeg nøye meg med å gå nærmere inn på to mulige forklaringer.

Norsk forvaltningspolitikk er i stor grad preget av ønsket om å utvikle elektroniske løsninger. Som nevnt i innledningen er eForvaltning et mangfoldig fenomen, som bl.a. gjelder forholdet mellom borgere/næringsliv og

18 Se Bygrave, Lee A.; Schartum, Dag Wiese:»Consent, Proportionality and Collective Power», I: *Reinventing Data Protection?,* Springer Science+Business Media B.V. 2009, s. 157-173.

19 Se Knut S Selmer: «Det stramme samfunn» (s 35) i RD Blekeli og KS Selmer (red), *Data og personvern* (Oslo, Universitetsforlaget, 1977) s 27 – 39, som benevner dette «borgervennlig administrasjon».

20 Se Dag Wiese Schartum og Lee A. Bygrave: «Personvern i informasjonssamfunnet», (Bergen, Fagbokforlaget, 2004) s 70 flg.

21 Enkelte gav i stedet tilgang til spesielle grupper av arbeidstakere (informasjonsmedarbeidere, ledere mv).

forvaltningsorganer i tilknytning til tjenesteyting og myndighetsutøvelse (jf figur 1, ovenfor). I regjeringens Stortingsmelding fra 2009 om den fremtidige forvaltningspolitikken, fremheves det at IKT gjør det mulig å automatisere forvaltningen, og at slik automatisering legger til rette for selvbetjeningsløsninger.[22] En selvbetjent forvaltning har positive begrunnelser som særlig gjelder økt tilgjengelighet til forvaltningen kombinert med kostnadseffektivisering. Begrunnelsen for selvbetjening kan imidlertid alternativt formuleres «negativt». For eksempel kan en begrunnelse være at den direkte og individuelle kommunikasjonen med den enkelte borger er uforholdsmessig dyr, og at den derfor bør erstattes med billigere, IKT-baserte rutiner. Slik kan selvbetjeningsløsninger også ses som uttrykk for ønske om en forvaltning som i mindre grad enn tidligere forutsetter direkte personlig tilgang til sine ansatte, og i større grad er basert på hjelp til selvhjelp for borgerne. For å tilrettelegge for selvbetjening er det om å gjøre at bildet av forvaltningen ikke er så komplisert at det blir en hindring for å finne fram. Derfor blir det understreket at borgere som benytter selvbetjente løsninger ikke trenger å vite hvordan forvaltningen er organisert. I stedet lages de digitale systemene slik at forvaltningen framstår som helhetlig og samordnet.[23]

I tillegg til at direkte kommunikasjon med enkeltmennesker er dyrt og selvbetjeningsløsninger billige, kan reduksjon av direkte kommunikasjon mellom borgere og ansatte i forvaltningen også begrunnes i fare for at slik kontakt vil gi ufullstendige journaler og arkiver. Forvaltningen har en plikt til journalføring og arkivering.[24] Elektronisk post som sendes sentrale postmottak («post@forvaltningsorgan.no») kommer til arkivet som har journalføring og arkivering som sin spesialiserte oppgave. Dersom elektronisk post går direkte mellom borgerne og den enkelte saksbehandler, innebærer det en fare for at saksbehandler lar være å journalføre og arkivere. Hensynet til registrering av inn- og utkomne saksdokumenter mv, kan derfor sies å tale mot direkte kommunikasjon mellom ansatte og borgere. Positivt uttrykt kan hensynet til offentlighet i forvaltningen tale for at elektronisk kommunikasjon skjer direkte til/fra sentrale postmottak.

22 Se St.meld. nr. 19 (2008-2009), «Ei forvaltning for demokrati og fellesskap», avsnitt 2.4.8. Andre steder i meldingen framheves det imidlertid at enkelte forvaltningsområder ikke egner seg for automatisering.

23 Se St.meld. nr. 17 (2006-2007) «Eit informasjonssamfunn for alle», avsnitt 7.3.1.

24 Se arkivloven LOV-1992-12-04-126 § 6, (arkivplikt), samt forskrift om offentlege arkiv av 11. desember 1998 nr 1193 § 2-6, jf offentleglova av 19. Mai 2006 nr 15 § 10 (journalføringsplikt).

Norske regler om arbeidsgivers adgang til å åpne ansattes elektroniske post mv, styrker dette argumentet. Etter reglene i personopplysningsforskriften[25] kapittel 9 har arbeidsgivere (også i offentlig forvaltning) bl.a. rett til og aksessere ansattes epost og filer dersom dette er «nødvendig for å ivareta den daglige driften eller andre berettigede interesser».[26] Vilkåret for tilgang er riktignok skjønnsmessig og ikke særlig strengt. Av større betydning er det imidlertid at åpning av slik epost bare kan skje i samsvar med framgangsmåter som er fastsatt i forskriftens § 9-3. Jeg vil ikke her komme nærmere inn på hvilke prosessuelle krav som gjelder, men nøyer meg med å understreke at kravene gjør at tilgang innebærer tidsforsinkelse og arbeidsinnsats. Epost med saksdokument mv som ved en feil kun havner i den ansattes epostkonto, blir derfor i praksis meget vanskelig tilgjengelig for forvaltningsorganet, og det er derfor av betydning å påse at dette ikke skjer.

I undersøkelsen av eksponeringen av ansatte på offentlige nettsteder, stilte vi flere spørsmål til ansatte som det var publisert epostadresse til hvorledes de håndterte henvendelser som kom direkte til dem på deres personlige adresse. Blant annet spurte vi i hvilken grad de journalførte *inngående* epost fra brukere/parter? Ca 25 % svarte at det nesten aldri skjedde eller ikke var aktuelt med slik journalføring, ca 41 % gjorde det av og til, og ca 32 % journalførte slik epost ofte. Vi spurte også i hvilken grad respondentene journalførte epost når de sendte *utgående* henvendelser til brukere/parter fra sin epostadresse på jobben? For ca 29 % av de som svarte skjedde dette nesten aldri eller var ikke aktuelt, ca 43 % gjorde det av og til, mens ca 28 % journalførte ofte.

Til begge de nevnte spørsmålene var det mange respondenter som understreket at eposten måtte være journalføringspliktig. Selv om det er usikkert om alle som svarte la en slik forutsetning til grunn, gir undersøkelsen trolig grunnlag for å hevde at en forholdsvis stor andel av inn- og utgående eposthenvendelser som går direkte mellom borgere og ansatte, ikke blir journalført slik de skal. Er dette riktig, er det åpenbart et relevant argument for ikke å tillate slik direkte kommunikasjon med epost, og i stedet påby at all slik post går via egne postmottak. En annen løsning kan være å forby ansatte å bruke sin epostadresse i jobben til private formål, slik at alle innkomne eposter kan sendes til og behandles i arkivet.[27]

En tredje strategi vil være å forbedre de teknologiske og organisatoriske løsningene for å gjøre det mindre tid- og ressurskrevende å arkivere slike hen-

25 Forskrift av 15.desember 2000 nr 1265.

26 Se § 9-2 første ledd bokstav a.

27 En slik løsning vil åpenbart være problematisk for personvernet fordi personer som sender inn epost til personlige adresser ikke alltid vil vite at henvendelsen vil bli lest av arkivet.

vendelser. I undersøkelsen spurte vi således om hvor tidskrevende respondentene synes det er å journalføre inn- og utgående epost til/fra sin epostadresse. I alt 41,7 % mente det var lite tidkrevende, mens 40,4 % svarte «noe tidkrevende». Hele 17,9 % gav imidlertid uttrykk for at slik journalføring var «veldig tidkrevende», og flere gav merknader som uttrykte frustrasjon over den praktiske situasjonen. Tallene gir grunn til å tro at manglende journalføring i stor grad inntreffer der denne er veldig eller noe tidkrevende. Nyere journalføringssystemer peker imidlertid i retning av at dette vil bli et stadig mindre problem etter hvert som forvaltningen moderniserer sine systemløsninger.

5 Avslutning

Selv om det forrige avsnittet minner oss om at det er argumenter som trekker i retning av å begrense den direkte kontakten mellom borgerne og ansatte i forvaltningen, er argumentene som taler for en slik kontakt etter min mening klart mer tungtveiende. Som nevnt tilsier hensynet til den enkelte borgers personvern at det er mulig å komme i kontakt med en person som kan gi informasjon og veiledning om den konkrete behandlingen av opplysninger om vedkommende. Når personopplysninger behandles som ledd i myndighetsutøvelse, gjør hensynet til rettssikkerhet argumentet for tilgang til forvaltningens ansatte sterkere. Særlig gjelder dette i saker som anses som vanskelige, og ellers der det er konflikt mellom borgeren og forvaltningsorganet. I slike situasjoner er det nemlig behov for å argumentere i egen sak og generelt bli så godt orientert som mulig om den rettslige reguleringen mv. Dette behovet kan imidlertid ikke begrunne at enhver saksbehandler i forvaltningsorganet skal være tilgjengelig for personlig kontakt. Forvaltningens menneskelige ansikt kan derfor primært tenkes tilgjengelig på «brukersentra», «servicekontorer» mv, dvs. enheter med bred kompetanse som kan svare på spørsmål som ikke krever spesialistkunnskap. Forutsetningen må i så fall være at slike generalister i førstelinjen alltid må kunne formidle kontakten videre direkte til spesialister, slik at borgeren alltid kan velge å oppsøke en person som har tilstrekkelig kompetanse.

I elektronisk forvaltning er det viktig å diskutere hva som er gode elektroniske løsninger, hvilken grad av automatisering som bør velges, og hvilken grad og på hvilken måte den enkelte borger bør involveres i ulike IKT-baserte selvbetjeningsrutiner. På ganske mange forvaltningsområder tror jeg det – i alle fall på sikt – er rom for å gå ganske langt i retning av saksbehandlingsrutiner der det i det store flertallet av saker ikke skjer noen medvirkning fra eller kontakt med saksbehandlere. Uansett hvor avanserte og automatiserte vi gjør forvaltningens informasjonssystemer, og uansett hvor store deler av befolkningen det er mulig å ha som aktive brukere av elektronisk forvaltning, vil

det imidlertid alltid være rom for og behov for en menneskelig faktor. Derfor er det viktigste og mest urovekkende resultatet fra den refererte undersøkelsen om tilgangen til kontaktopplysninger om ansatte i norsk forvaltning, at *mer enn 60 %* av de undersøkte kommunene og statsetatene[28] over hode *ikke* hadde gjort slike kontaktopplysninger tilgjengelige.

28 Henholdsvis 62 % i kommunene og 73 % i statsetatene.

INFORMASJONSSIKKERHET OG PERSONVERN I SKOLEN[1]

Tommy Tranvik

Innledning

I løpet av noen få tiår har den tekniske utstyrssituasjonen i norsk skole endret seg radikalt. Dette kommer til uttrykk hvis vi ser på innholdet i en håndbok i praktisk skoleledelse publisert i 1978.[2] Her gir forfatterne en oversikt over hvilke teknisk hjelpemidler som de mener at rasjonell og effektiv administrasjonen av den moderne skolen forutsetter. De fremhever særlig viktigheten av å ha tilgang til diktafon,[3] telefon, hustelefonanlegg, elektronisk skrivemaskin, ulike typer kopimaskiner (enkeltkopier, bildekopier og sverteduplikater), hullmaskin, elektronisk stiftemaskin, kalender, arkivskap og safe. Til undervisningsformål anbefaler forfatterne musikkanlegg, film- og lysbildefremviser og tv-apparat.[4]

Hvis vi lager en tilsvarende oversikt over hva skoleadministrasjon og undervisning anno 2010 forutsetter av teknisk utstyr, er det ikke overraskende at listen ser annerledes ut (og er en god del lenger) enn den fra 1978.[5] Det er heller ikke overraskende at dette skyldes tre forhold:

---

1 Datagrunnlaget for denne artikkelen er tredelt, og datainnsamlingen skjedde i 2009-10. Først er den basert på over 70 intervjuer med aktører i skolesektoren fordelt på tre nivåer: nasjonalt nivå, skoleeiernivå og skolenivå. Dernest på deltakelse i risikovurderinger av informasjonssikkerheten i skolesektorens IT-systemer gjennomført i fire kommuner på det indre østlandsområdet. Til slutt på Datatilsynets rapporter fra tilsynsbesøk i skolesektoren gjennomført i perioden 2001-2010 (det vil si helt siden personopplysningsloven og forskriften trådte i kraft). Prosjektet ble finansiert av Senter for IKT i utdanningen.

2 Inger Lødrup og Torkel Sandvei (1978): Skoleleder i dag. En håndbok i praktisk skoleledelse. Oslo: NKS-Forlaget.

3 «Det går ikke lenge før man oppdager diktafonens fordeler, sammenliknet med håndskrevne notater og amatørmessig maskinskriving» (ibid: 36).

4 Det samme poenget kan illustreres gjennom et tankeeksperiment: Hvis vi plasserte en lærer fra 1880 i en tidsmaskin og flyttet vedkommende 100 år frem og tilbake i tid – til et klasserom i 1980 og i 1780 – ville han i begge tilfellene trolig kjent seg igjen og vært i stand til å utøve sitt yrke uten altfor store problemer. Men hvis vi flyttet 1880-tallslæreren til et klasserom anno 2010, ville han ikke bare vært ubehjelpelig i møte med det tekniske utstyret som finnes i dagens skole. Han ville også trolig hatt problemer med å forstå at han befant seg i et klasserom (i alle fall ved enkelte skoler).

5 Som følge av den siste store reformen av grunnutdanningen – Kunnskapsløftet og tilhørende læreplaner – har digital kompetanse blitt definert som én av fem basisferdigheter (se NOU

- enkelte typer utstyr har falt ut av listen (for eksempel elektronisk skrivemaskin, film- og lysbildefremviser og sverteduplikater),
- enkelte andre typer utstyr har beholdt sin plass (for eksempel telefon, hullmaskin og arkivskap),
- en rekke nye hjelpemidler, som ingen skoleleder, skoleadministrator, lærer, elev eller forelder anno 1978 ville visst hva er, har funnet sin vei inn på listen: skoleadministrative systemer, digitale læringsplattformer, e-post, spesialpedagogisk programvare, skytjenester, bærbare og stasjonære datamaskiner, Internett, identitetsforvaltningsløsninger, filservere, bredbånd, printere, osv.

Det som også har skjedd etter hvert som skolene har tatt i bruk disse og andre IT-løsninger, er at flere aktører utenfor skolen er involvert i selve skoledriften enn hva tilfelle var for godt og vel tre tiår tilbake. Den kommunale IT-avdelingen, interkommunale IT-selskaper eller driftssamarbeid og leverandører av IT-systemer er eksempler på dette.[6]

Forskjellene mellom 2010 og 1978 som er skissert ovenfor, er relativt lette å få øye på. Men de bringer samtidig med seg en rekke andre endringer som har fått liten oppmerksomhet i den norske skolen. Dette handler i første rekke om rettslige og praktiske utfordringer som elektronisk og datamaskinbasert behandling av opplysninger om lærere, administrativt ansatte, elever og foreldre fører med seg.[7]

I denne korte artikkelen vil jeg drøfte noen av disse utfordringene. Jeg vil rette fokuset mot kravene som lovgivningen på personopplysningsområdet stiller til informasjonssikkerhet.[8] Drøftelsen vil indikere at både grunn- og videregående skoler står overfor en rekke utfordringer når det gjelder å etterleve

---

2003: 16, *I første rekke*; St.melding nr. 30 (2003-04), *Kultur for læring*). Det innebærer at bruk av digitale hjelpemidler skal være en integrert del av undervisningen i alle fag og på alle nivåer. Dette har trolig bidratt til at skolenes investeringer i IKT har økt.

6 I 1978 var involveringen av eksterne aktører i den regulære skoledriften mer begrenset, og omfattet for eksempel skoleskysselskaper og lokale arbeidsplasser for utplassering av elever.

7 Problemstillinger knyttet til personvern i skolen ble også diskutert i den regjeringsoppnevnte personvernkommisjonens sluttrapport (se NOU 2009: 1, *Individ og integritet. Personvern i det digitale samfunnet*, kapittel 14).

8 Informasjonssikkerhet og personvern er en viktig del av den nasjonale e-forvaltningspolitikken, se for eksempel St. meld. Nr. 17, 2006-07, *Eit informasjonssamfunn for alle*, kapittel åtte og ni. I henhold til Fornyings og administrasjonsdepartementets *Nasjonale strategi for styrking av informasjonssikkerheten 2007-2010*, er skolesektoren en viktig aktør i denne sammenheng. Det nasjonale ansvaret for å ivareta strategien på skoleområdet, er tillagt Senter for IKT i utdanningen. I tillegg har informasjonssikkerhet og personvern fått en fremskutt plass i utviklingen av kommunale institusjoner, se *e-kommune 2012 – lokal digital agenda*, s. 22-23.

kravene til tilfredsstilende sikring av den store (og økende) mengden elektroniske personopplysninger som de er ansvarlige for.

Personopplysningsloven og informasjonssikkerhet

Personopplysningsloven med forskrift inneholder regler for behandling av personopplysninger som skjer ved bruk av elektroniske hjelpemidler.[9] Her defineres personopplysninger som alle former for informasjon eller vurderinger som er knyttet til identifiserbare personer.[10] Personopplysninger kan derfor foreligge i form av tekst, bilder, video eller lydopptak: alle disse mediene kan formidle personrelaterte vurderinger eller informasjon. De personopplysninger som skolen behandler elektronisk, og som derfor omfattes av reglene i personopplysningsloven og forskriften, kan deles inn i tre kategorier:

1. For det første det vi kan kalle for grunndata. Dette er grunnleggende opplysninger om elever, foreldre, lærere og andre ansatte som skolen trenger til administrative formål (for eksempel navn, fødselsnummer, elevens og foreldrenes bostedsadresse, elevens eller foreldrenes telefonnummer, trinn/klasse, osv.). Grunndata registreres i såkalte kildesystemer, for eksempel skoleadministrative systemer eller lønns- og personalsystemer, men enkelte av dem kan også inngå i manuelle personregistre (bl.a. i elevmapper).
2. For det andre det vi kan kalle for tjenesterelaterte data. Dette er opplysninger som pedagogisk og administrativt ansatte registrerer om skolens brukere (elever og foreldre) ved utførelsen av de oppgaver som opplæringsloven pålegger skolen å ivareta (for eksempel fravær, karakterer, anmerkninger, faglig progresjon, spesielle undervisningsbehov, adferdsmønstre, sosiale ferdigheter, osv.). Enkelte av disse opplysningene registreres i kildesystemer (fravær og karakterer), men vanligere er det at de behandles i andre informasjons- og IT-systemer (for eksempel digitale læringsplattformer, bærbare eller stasjonære lærer-pc-er, skolens filservere, osv.).
3. For det tredje det vi kan betegne som brukergenererte data. Dette er opplysninger som skolens brukere enten er pliktig til eller frivillig registrerer i skolens informasjons- og IT-systemer (for eksempel prøver/oppgaver, elevarbeider, e-posthenvendelser, elektroniske meldinger, osv.). Brukergenererte data omfatter også opplysninger som registreres av skolens informasjons- og IT-systemer. Dette kan for eksempel være aktivitets-

9 Den norske loven og forskriften trådte i kraft fra 1. januar 2001, og baserer seg på EUs personverndirektiv fra 1995 (Direktiv 95/46/EF).

10 Jf. personopplysningsloven § 2. Informasjon eller vurderinger som i utgangspunktet ikke er knyttet til en identifisert person vil derfor være personopplysninger hvis det er mulig å finne ut hvem denne personen er.

logger, feilmeldingslogger, osv. Slike data registreres når brukerne benytter eller forsøker å nå IT-systemene.[11]

Det er behandlingen av disse tre typene personopplysninger som personopplysningen med forskrift tar sikte på å regulere. Lovverket inneholder regler om hvilke vilkår som må oppfylles for at skoleeiers behandling av personopplysninger skal være lovlig og hvilke rettigheter de registrerte (elever, foreldre lærere og andre ansatte) har når skoleeier bruker opplysningene.[12] I tillegg inneholder personopplysningsloven § 13 og personopplysningsforskriften kapittel to krav til hvordan skoleeier og skolen skal sikre opplysningene. Her er kravet at personopplysningene sikres på en tilfredsstillende måte. Tilfredsstillende sikring innebærer at skolen eller skoleeier skal iverksette tiltak for å hindre:

- brudd på personopplysningenes konfidensialitet, det vil si uautorisert innsyn i opplysninger om den enkelte elev, foreldre eller ansatt,
- brudd på personopplysningenes integritet, det vil si uautorisert endring av opplysninger om den enkelte elev, foreldre eller ansatt,
- brudd på personopplysningenes tilgjengelighet, det vil si å unngå at de som har legitime behov for tilgang til opplysninger om den enkelte elev, foreldre eller ansatt ikke får tak i opplysningene når de trenger dem.[13]

Hensikten med å hindre brudd på informasjonssikkerheten er å unngå krenkelser av grunnleggende personvernhensyn, bl.a. privatlivets fred og den personlige integriteten. Prinsippet i personopplysningsloven og forskriften er at den registrerte (vedkommende som opplysningene gjelder, for eksempel læreren, eleven eller foreldrene) skal ha en viss kontroll med og innflytelse over hvordan skolen og skoleeier anvender deres personopplysninger.[14] Personvernkrenkelser handler derfor om at skolen eller skoleeier ikke er i stand til å ivareta den registrertes rett til opplysningskontroll og innflytelse. I forhold til informasjons-

11 Aktivitetslogger kan for eksempel registrere hvem som har åpnet hvilke elektroniske dokumenter, når og hvor lenge dokumentene har vært åpnet, osv.

12 Skoleeier er såkalt behandlingsansvarlig, det vil si at pliktene i personopplysningsloven og forskriften retter seg mot kommuner og fylkeskommuner. Men i praksis vil det i stor grad være hver enkelt skole som må sørge for at pliktene blir ivaretatt.

13 For ulike perspektiver på rettslig regulering av informasjonssikkerhet, se Arild Jansen og Dag Wiese Schartum (red.) (2005): *Informasjonssikkerhet. Rettslige krav til sikker bruk av IKT*. Bergen: Fagbokforlaget.

14 Denne forståelsen av hva personvernkrenkelser ved behandling av personopplysninger dreier seg om ble først formulert av Alan Westin: «Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how and to what extent information about them is communicated to others» (Alan Westin (1967): *Privacy and Freedom*. New York: Atheneum, side 7).

sikkerhet kan dette skje hvis skolen ikke greier å hindre at (i) opplysninger om elever eller foreldre eksponeres for uvedkommende (konfidensialitetsbrudd), (ii) det skjer uautorisert endring av personopplysninger slik at de gir et misvisende eller feilaktig bilde av eleven eller læreren (integritetsbrudd) eller (iii) elever og foreldre ikke får innsyn i hvilke opplysninger som skolen har om dem fordi opplysningene er utilgjengelige (tilgjengelighetsbrudd).

Denne typen krenkelser av personvernet som følge av brudd på opplysningenes konfidensialitet, integritet og tilgjengelighet, kan sies å være spesielt viktig å unngå (så langt det er mulig) i skolen. Det skyldes tre forhold. For det første fordi mange av opplysningene gjelder personer (elever) som ikke alltid kan forventes å ivareta sine personverninteresser på egen hånd. Dermed blir det i stor grad opp til skolen og skoleeier å sikre opplysningene mot krenkelser av personvernet. For det andre fordi opplæringsplikten gjør at elever (og foreldre) i grunnskolen ikke kan velge om de ønsker å overlate personopplysninger i skolens varetekt: de plikter å gi fra seg personopplysninger uavhengig av hva skolen har gjort for å sikre opplysningene. For det tredje fordi personopplysninger som skolen forvalter også omfatter foreldre og hjemmeforhold. Det fører til at de personvernmessige konsekvensene av eventuelle brudd på informasjonssikkerheten fremstår som potensielt alvorlige. Til sammen gjør disse tre forholdene at skolen og skoleeier kan hevdes å ha et spesielt ansvar for å sørge for sikker behandling av personopplysninger.

Mens de øvrige pliktene i personopplysningsloven og forskriften retter seg mot skoleeier (kommunen eller fylkeskommunen) som sådan, er det rådmannen som har ansvaret for at informasjonssikkerheten er tilfredsstillende.[15] Rådmannen har også ansvaret for å bestemme hva som menes med tilfredsstillende informasjonssikkerhet – dette er en rettslig norm som må operasjonaliseres i hver enkelt kommune eller fylkeskommune. Ut over å bestemme det konkrete meningsinnholdet i denne rettslige normen, er det vanligvis slik at deler av det konkrete sikkerhetsarbeidet delegeres fra rådmannen til rektorene (virksomhetslederne).[16] Den viktigste av disse delegerte oppgavene, er ansvaret for gjennomføring av risikovurderinger.[17]

15 «Den daglige ledelsen av virksomheten som den behandlingsansvarlige driver» (personopplysningsforskriften § 2-3).

16 Hvem som har ansvaret for å utføre hvilke sikkerhetsoppgaver er vanligvis beskrevet i den kommunale sikkerhetshåndboken. Se også Tommy Tranvik (2009): *Personvern og informasjonssikkerhet. En studie av rettsreglers etterlevelse i kommunal sektor*. Complex 4/09, Senter for rettsinformatikk.

17 Jf. personopplysningsforskriften § 2-4.

Risikovurderinger er en standard arbeidsmetodikk i sikkerhetssammenheng.[18] Slike vurderinger innebærer at skolen kartlegger sannsynligheten for og konsekvensene av brudd på opplysningenes konfidensialitet, integritet og tilgjengelighet: hvor sannsynlig er det at det som kan gå galt går galt og hvor ille kan det da gå? Hvis risikoen for sikkerhetsbrudd vurderes å være for høy (stor sannsynlighet, alvorlige konsekvenser eller begge deler), plikter skolen å iverksette tiltak for å beskytte personopplysningene bedre.

Nedenfor vil jeg gi en kort gjennomgang av noen av de viktigste IT-systemene i skolen. Her vil jeg vise eksempler på hvilke sikkerhetsproblemstillinger som bruken av systemene kan føre med seg og skissere enkelte utfordringer knyttet til etterlevelsen av reglene om informasjonssikkerhet i dagens lovverk. Til slutt vil jeg rette fokuset mot viktige ikke-teknologiske faktorer og utviklingstrekk som synes å påvirke både personvern- og sikkerhetstilstanden i skolen og skolens muligheter for å etterleve reglene om sikring av personopplysninger.

Elektronisk infrastruktur

Kommunens elektroniske nettverk er som regel delt opp i to fysisk atskilte nett: administrasjonsnettet og elevnettet. Administrasjonsnettet har skolens ansatte tilgang til (private mapper, fellesområder, osv.) mens elevene (og foreldre) har tilgang til digitale ressurser på elevnettet (læringsplattform, e-post, pedagogisk programvare, osv.).

Det er også standard at administrasjonsnettet er inndelt i ulike sikkerhetssoner (basert på råd gitt i veileder i informasjonssikkerhet for kommuner og fylkeskommuner utgitt av Datatilsynet[19]). Det vanlige er at tjenesterelaterte data av sterkt personlig eller sensitiv karakter (for eksempel opplysninger om elever med behov for spesielt tilrettelagt undervisning) behandles i sikker sone, mens ikke-sensitive opplysninger behandles i intern sone.[20] Brukergenererte data, og de verktøyene som anvendes til å produsere disse dataene (tekstbehandlingsverktøy, regneark, pedagogisk programvare, osv.), behandles på elevnettet.

Mange av sikkerhetsutfordringene som knytter seg til skolens elektroniske infrastruktur, spesielt administrasjonsnettet, er ikke spesifikke for skolesektoren. Tilsvarende utfordringer vil vi også finne igjen i andre offentlige institusjoner eller private bedrifter. Det gjelder for eksempel muligheten for å bli utsatt

18 Se for eksempel ISO/IEC 27002: *Information Technology – Security Techniques – Code of Practice for Information Security Management* eller Datatilsynet (2002): *Risikovurdering av informasjonssikkerhet*.

19 Datatilsynet (2005): *Veiledning i informasjonssikkerhet for kommuner og fylker*.

20 Se Datatilsynet (2005): *Veiledning i informasjonssikkerhet for kommuner og fylker*, s. 25-31.

for eksterne dataangrep som kan føre til at IT-systemene blir utilgjengelige for en periode, eller at svakheter i nettverket gjør at datatrafikken (for eksempel e-post) snappes opp og leses av uvedkommende. Den tekniske kompleksiteten i nettverk og nettverksutstyr kan i tillegg føre til at uvedkommende får tilgang til opplysninger om elever, foreldre, lærere og andre ansatte fordi de IT-ansatte (i en travel hverdag) har mistet oversikten over hvordan alle delene i nettverket fungerer sammen. En annen typisk sikkerhetsutfordring er at oppdateringer av programvare som har en kjent sårbarhet ikke blir gjort. Dermed kan uvedkommende komme seg inn på beskyttede nettverksområder (sikker sone) og endre, slette eller hente ut sensitive og ikke-sensitive personopplysninger.

Det knytter seg i tillegg visse utfordringer til bruken av de lagringsområdene som skolens ansatte får tilgang til på administrasjonsnettet (private mapper og fellesområder). Et typisk problem her er for eksempel at sterkt personlige opplysninger om enkeltelever (bl.a. problematferd) lagres på fellesområdet istedenfor i lærerens private mappe. Dermed kan ansatte ved skolen som ikke har tjenestelige behov for å kjenne til opplysningene likevel få tilgang til dem. Det er heller ikke en ukjent problemstilling at dokumenter med sensitive personopplysninger kopieres fra lærernes private mappe og over på minnepenner, som læreren tar med seg hjem for å jobbe videre med på sin egen datamaskin. På denne måten øker sannsynligheten for at sensitive opplysninger kommer på avveier (bl.a. ved at minnepinne mistes/stjeles).

Oppdelingen av den elektroniske infrastrukturen i et administrasjons- og et elevnett, er i seg selv et sikkerhetstiltak. Oppdelingen skal bl.a. bidra til å unngå at elever eller foreldre – tilsiktet eller utilsiktet – henter ut, endrer eller forhindrer tilgangen til personopplysninger som er skjermet og som skolens ansatte trenger i sitt arbeid. Utfordringen her vil typisk være å unngå at det finnes en bro mellom nettverkene, det vil si en elektronisk kanal fra elev- til administrasjonsnettet. En slik bro kan for eksempel skapes hvis IT-systemer som elevene benytter (kanskje spesielt digitale læringsplattformer) ligger på datamaskiner som er tilknyttet administrasjonsnettet. Hvis det er tilfelle, kan elever eller foreldre få tilgang til dataressurser og personopplysninger som nettverksoppdelingen i utgangspunktet tok sikte på å forhindre.

Skoleadministrative systemer

Skoleadministrative systemer (for eksempel Oppad og Extens) er kildesystemer hvor skolen registrerer grunndata om elever og foreldre. De benyttes i tillegg til registrering av visse typer tjenesterelaterte data, for eksempel karakterer, fravær/fraværsmerknader og elevvurderinger.

Grunndata importeres fra Folkeregistret eller innsamles og registreres manuelt av det administrative personalet, mens pedagogisk personale (kontaktlærer og faglærere) registrerer og oppdaterer tjenesterelaterte data. Rektorene spiller også en rolle i forhold til de skoleadministrative systemene, bl.a. når det gjelder å legge opp timeplaner og eksport av grunndata til nasjonale registre.[21]

Typiske sikkerhetsutfordringer i forhold til skoleadministrative systemer, er at de vanligvis ikke befinner seg innenfor sikker sone i kommunens administrasjonsnettverk. Dermed skal bare ikke-sensitive elevopplysninger registreres i disse systemene. Systemene er, ifølge Datatilsynet,[22] ikke godt nok beskyttet mot sikkerhetsbrudd til at registrering av sensitiv elevinformasjon godtas.[23] Til tross for dette er det flere forhold som kan føre til at de skoleadministrative systemene likevel behandler sensitive personopplysninger.

For det første ved at systemene kan være lagt opp slik at de «oppmuntrer» til registrering av denne typen opplysninger. Når det føres fravær kan systemene for eksempel tilby menyvalg for registrering av hvilke typer fravær det er snakk om (gyldig, ugyldig, sykdom, osv.). Samtidig er det ikke uvanlig at systemene inneholder fritekstfelt hvor lærerne eller administrativt ansatte kan gjøre notater i tilknytning til elevenes fravær. Det betyr at hvis alternativet «sykdom» velges fra menylisten og fritekstfeltet benyttes til å utdype hva dette innebærer, kan skolen registrere sensitive elevopplysninger (helsedata) i et IT-system hvor sikkerheten er for dårlig til at dette godtas.

For det andre ved at det legges inn opplysninger fra Folkeregistret som ikke er korrekte (manglende oppdatering). Feil i datagrunnlaget fra Folkeregistret kan for eksempel føre til at personer som ikke lenger har foreldreansvaret likevel blir stående oppført som foreldre i skolens IT-system, og dermed blir tilsendt informasjon fra skolen.[24] I verste fall kan dette lede til at foreldre og barn som lever på skjermet adresse (som den andre forelderen ikke skal få kjennskap til) får sin bostedsadresse kompromittert. For det tredje ved at skolens egne ruti-

21 For eksempel til opptakssystemet for videregående opplæring – VIGO – og til det prøveadministrative systemet som Utdanningsdirektoratet anvender ved gjennomføringen av nasjonale prøver.

22 Datatilsynet (2005): *Veiledning i informasjonssikkerhet for kommuner og fylker*.

23 Det er også vanlig at skolene har laget interne rutiner som forbyr registrering av sensitive elevopplysninger i det skoleadministrative systemet.

24 Mange skoler får derfor enkelte av sine grunndata, for eksempel foreldrenes bostedsadresse, fra Posten (folk er raskere til å melde adresseendringer til Posten enn til Folkeregistret). Men å skaffe seg informasjon om bortfall av foreldreansvar må skolene gjøre på egen hånd.

ner for registrering og oppdatering av opplysninger ikke følges.[25] Denne utfordringen kan innebære et tilsvarende brudd på opplysningenes konfidensialitet som ved feil i datagrunnlaget fra Folkeregistret: uvedkommende (for eksempel tidligere samboere) får informasjon fra skolen om eleven fordi skolen ikke har fremskaffet oppdaterte opplysninger om elevens familieforhold. For det fjerde ved at det oppstår uklarheter rundt hvem som har registrert hva. Det kan for eksempel innebære at en elev blir stående oppført med for høyt fravær fordi kontaktlærer og faglærere har registrert det samme fraværet to (eller flere) ganger. Det kan diskuteres om dette er et brudd på opplysningenes integritet, det vil si at lærere som ikke har lov til å føre fravær på eleven gjør det likevel, eller om det skyldes andre forhold (for eksempel at lærere som har lov til å registrere fravær unnlater å koordinere sin fraværsføring). Uansett årsak må dette likevel betegnes som en personvernkrenkelse fordi de registrerte opplysningene gir et misvisende bilde av vedkommende elevs atferd.

En femte utfordring oppstår hvis skoleeier ikke drifter det skoleadministrative systemet selv, men har satt ut driften til en ekstern aktør (for eksempel leverandøren av systemet, en annen kommune eller et interkommunalt IKT-selskap). Her er den eksterne aktøren å betrakte som databehandler, det vil si at han behandler personopplysninger på vegne av skoleeier.[26] Ifølge lovverket skal det dermed foreligge en såkalt databehandleravtale mellom skoleeier og driftsoperatøren.[27] Av avtalen skal det bl.a. fremgå at driftsoperatøren plikter å følge reglene om informasjonssikkerhet i personopplysningsloven og forskriften, og at skoleeier kan be om innsyn i sikkerhetsarbeidet. Problemstillingen i slike situasjoner er vanligvis tredelt: (i) skoleeier og driftsoperatør har ikke undertegnet noen databehandleravtale; (ii) avtalen foreligger, men skoleeier følger den ikke opp (sjekker ikke at driftsoperatøren gjør det avtalen sier at han skal gjøre); (iii) sensitive personopplysninger overføres over Internett til ekstern driftsoperatør (for eksempel i forbindelse med fraværsføring), men

25 Det er meningen at brudd på interne rutiner skal fanges opp av en skoleeiers avviksmeldings- og håndteringssystem (etablering av et slikt system er en rettslig plikt, se personopplysningsforskriften § 2-6). Det betyr at de ansatte skal melde inn brudd på lokale rutiner slik at problemet kan utbedres. Svakheten med systemet er skoleeier mottar svært få meldinger om rutineavvik, både fra skolene og fra andre virksomheter (se også Tommy Tranvik (2009): *Personvern og informasjonssikkerhet. En studie av rettsreglers etterlevelse i kommunal sektor*. Complex 4/09, Senter for rettsinformatikk).

26 Skoleeier er fortsatt behandlingsansvarlig, det vil si at skoleeier sitter med det rettslige ansvaret for opplysningene. Det innebærer bl.a. at skoleeier er erstatningsansvarlig hvis lærere, elever eller foreldre lider overlast som følge av sikkerhetsbrudd hos den eksterne driftsoperatøren.

27 Jf personopplysningsloven § 15.

uten at overføringen er lovmessig sikret (manglende kryptering). Alle disse tre scenarioene representerer brudd på reglene om sikring av personopplysninger.

Digitale læringsplattformer

Det finnes mange ulike digitale læringsplattformer og de tilbys av kommersielle leverandører. De mest brukte læringsplattformene i norsk skole er it's learning, Class Fronter, PedIt, Microsoft Learning Gateway og Moodle. Læringsplattformer er virtuelle læringsmiljøer som inneholder en rekke undervisnings-, kommunikasjons- og publiseringsverktøy. De kan for eksempel brukes til utlevering og innlevering av oppgaver, gjennomføring av prøver, kommunikasjon elev-til-elev, lærer-til-elev og lærer-til-lærer, formidling av informasjon fra skolen til foreldre, formidling av informasjon fra ledelsen til lærere og andre ansatte, deling av undervisningsopplegg, generering av nettsider, blogging, osv.

I læringsplattformene kan det opprettes fellesområder («klasserom») som lærerne administrerer, og både lærere og elever kan få tilgang til private mapper/filområder. Denne e-forvaltningstjenesten inneholder derfor både tjenesterelaterte og brukergenererte data.[28] I tillegg til skolens ansatte og elever, kan også foreldrene ha tilgang til tilrettelagt informasjon på læringsplattformene.[29]

Digitale læringsplattformer representerer en særlig utfordring når det gjelder å oppfylle lovverkets (personopplysningsloven og forskriften) krav om tilfredsstillende informasjonssikkerhet. Som antydet ovenfor, skyldes dette at læringsplattformene kan benyttes til mange ulike formål og at de derfor inneholder en lang rekke muligheter for registrering, lagring, oppdatering, sletting, publisering og annen behandling av personopplysninger.[30] Dessuten er det

28 Plattformene inneholder også grunndata for å holde orden på brukerne (lærere, elever, osv.), men disse overføres fra det skoleadministrative systemet.

29 Hvilken informasjon foreldrene skal få tilgang til i forhold til egne barn, er et uavklart spørsmål – og oppfatningene er delte. Rettslig sett er et av hovedproblemene at elevene har krav på personvern i forhold til sine foreldre, men samtidig må foreldrene kunne ivareta sitt foreldreansvar på en hensiktsmessig måte (i tillegg sier § 1 i opplæringsloven at skolens virksomhet skal skje i samarbeid med hjemmet). Problemet består derfor i å avgjøre hva foreldrene skal ha tilgang til og hva som bør skjermes mot foreldreinnsyn. Her ser det ut til at skolenes praksis varierer en god del, men karakterer og fravær er opplysninger som foreldrene typisk får innsyn i. Det er også vanlig at foreldrene ikke får innsyn i personlig kommunikasjon elever imellom. Det samme gjelder kommunikasjon mellom lærer og elev.

30 Dette betyr at læringsplattformene kan være problematiske i forhold til et av de sentrale prinsippene i dagens personopplysningslovgivning: formålsprinsippet. Dette prinsippet innebærer at skolen må oppgi et konkret formål for behandlingen av personopplysninger (for eksempel skoleadministrasjon, undervisning, skole-hjem-samarbeid, intern eller ekstern informasjonsformidlige, personlig kommunikasjon, osv.). Bare opplysninger som er relevante

mange brukeraktører (ledere, lærere, elever, foreldre) som gis tilgang til innholdet på læringsplattformene. Dette øker utfordringen med å sikre at opplysningene ikke eksponeres for uvedkommende og at de ikke endres av personer som ikke har lov til å foreta endringer (for eksempel at foreldre retter feil eller gjør tilføyelser i oppgavebesvarelser som elevene jobber med slik at besvarelsene er en refleksjon av foreldrenes ambisjoner snarere enn elevenes ferdighetsnivå).

Den mest alvorlige (og åpenbare) sikkerhetsutfordringene, er imidlertid at brukernavn og passord kommer på avveier. Dette kan føre til at uvedkommende får tilgang til private kontoer på læringsplattformene og tilgangen kan benyttes til å endre, registrere eller formidle personopplysninger i en annen persons navn. Slik uautorisert behandling av personopplysninger betegnes gjerne som identitetstyveri, for eksempel at en elev tilegner seg klassekameratens konto og sender e-post eller andre elektroniske meldinger som mottakeren (feilaktig) tror kommer fra kontoens rettmessige innehaver (den rettmessige innehaveren kan da få store vansker med å bevise at det ikke var han som stod bak meldingene). Det samme kan skje hvis lærerens brukernavn og passord faller i hendene til en elev. Da kan eleven bl.a. få tilgang til lærerens private mapper som kan inneholde elevvurderinger av sensitiv eller sterkt personlig karakter.[31]

Det finnes dessuten en rekke andre sikkerhetsutfordringer knyttet til bruken av digitale læringsplattformer. Det kan for eksempel tenkes at læreren ved en feiltakelse gir alle lærerne tilgang til konfidensielle elevopplysninger, eller at elever utilsiktet offentliggjør sensitive personopplysninger om seg selv på Internett (for eksempel elevarbeider som indikerer en diagnostisk tilstand: dysleksi). Samtidig kan nye brukere (lærere, elever eller foreldre) få tildelt en feil rolle i systemet (for eksempel at elev registreres som lærer eller administrator) slik at de får innsyn i personopplysninger som skulle vært skjermet. Videre kan det tenkes at elever som har sluttet ved skolen ikke slettes som brukere, men fortsatt har tilgang til fellesområder hvor tidligere klassekamerater registrerer personopplysninger. Det finnes også en rekke andre muligheter for utilsiktet offentliggjøring av sensitive eller sterkt personlige elevopplysninger, og for feilaktig sletting av brukere som skulle hatt tilgang til plattformen (risikoen for

for formålet kan behandles. Såkalt overskuddsinformasjon – opplysninger som ikke er relevante for det oppgitte formålet – er det ikke lov å behandle. Spørsmålet blir da hva formålet med læringsplattformene er? I den grad dette er uklart, eller plattformene kan benyttes for en rekke ulike formål, kan det være vanskelig å avgjøre hvilke opplysninger som behandles lovlig og hvilke som må betraktes som overskuddsinformasjon.

31 Det forutsetter at læreren lagrer sensitive personopplysninger utenfor sikker sone. Funnene i dette prosjektet tyder på at det ikke er uvanlig (se også diskusjon ovenfor).

denne typen utilsiktede sikkerhetsbrudd er økende desto svakere lærernes eller administrativt ansattes dataferdigheter er).[32]

Det er heller ikke uvanlig at digitale læringsplattformer driftes av eksterne aktører (spesielt leverandører). Hvis dette er tilfelle, vil de samme problemstillingene som ble diskutert i forhold til ekstern drift av skoleadministrative systemer (inngåelse og oppfølging av databehandleravtale; sikker overføring av sensitive personopplysninger) dukke opp igjen. Forskjellen er at digitale læringsplattformer både benyttes til mange flere formål enn de skoleadministrative systemene og at de brukes av flere aktørgrupper (ledere, lærere, elever og foreldre). Dermed kan sjansen øke for at sensitive eller sterkt personlige opplysninger overføres fra skolen til driftsoperatøren uten at sikkerheten er lovmessig ivaretatt (manglende kryptering av overføringen).[33]

Identitetsforvaltningstjenester

Feide (Felles elektronisk identitet) er Kunnskapsdepartementets foretrukne innloggingsløsning for skolesektoren (Feide benyttes også ved universiteter og høyskoler).[34] Ved bruk av Feide får elever og lærere tildelt et brukernavn og passord som så benyttes til innlogging på ulike skoleinterne IT-systemer (for eksempel den digitale læringsplattformen) og eksterne webtjenester tilrettelagt for undervisningsformål (for eksempel NRK Skole, TV2 Skole, Kunnskap.no, Salaby, Viten.no, osv.).[35] Selve innloggingstjenesten driftes av Uninett i Trondheim, men det er skolene selv som må sørge for å ha god orden i og høy kvalitet på de grunndata som sikker Feide-innlogging forutsetter (navn, bostedsadresse, fødselsnummer, basisgruppe og enkelte andre opplysninger).[36]

---

32 En problemstilling som ble nevnt i flere intervjuer (og som Datatilsynet har vært opptatt av), er lærernes bruk av læringsplattformen til fagforeningsaktiviteter. Ifølge personopplysningsloven § 2, er opplysninger om enkeltpersoners fagforeningsvirksomhet å regne som sensitive. Men når læringsplattformene benyttes til fagforeningsvirksomhet, for eksempel utsending av møteinnkallinger, møtepapirer og referater, er sjansen relativt stor for at uvedkommende (for eksempel skoleledelsen) får tilgang til opplysningene.

33 Datatilsynet har gjennomført to tilsynsrunder rettet mot skolens bruk av digitale læringsplattformer. Begge gangene var et av hovedtemaene for tilsynet skolenes anvendelse av aktivitetslogger (som registrerer brukernes aktivitetsmønster). Ved siste tilsynsrunde uttrykte Datatilsynet tilfredshet med at aktivitetsloggene i liten grad ble brukt i de kontrollerte skolene. Se *Datatilsynets årsmelding 2009*, s. 39.

34 Se for eksempel Uninett ABC: *Krav til en vertsorganisasjon i Feide*.

35 Feide er basert på såkalt Single Sign-On (SSO). Det betyr for eksempel at hvis skolen har Feide-innlogging på sin digitale læringsplattform, kan elever og lærere som er innlogget gå direkte inn i NRK Skole uten å måtte taste inn sitt brukernavn og passord på nytt.

36 Dette er grunndata som skolene registrerer i sitt skoleadministrative system (se ovenfor).

Feide er en sikkerhetsteknologi på minst to måter.[37] For det første ved at Feide sørger for tilgangsstyring, det vil si at riktig person får tilgang til sine egne (og ingen andres) personopplysninger (og andre digitale ressurser). Feide (som andre identitetsforvaltningstjenester) bidrar derfor til å unngå konfidensialitets- og integritetsbrudd (riktig person får tilgang til og kan registrere, endre eller slette personopplysningene).[38] For det andre ved at Feide gjør at brukerne ikke trenger å huske mange forskjellige og tjenestespesifikke brukernavn og passord – én nøkkel åpner mange dører istedenfor at brukerne trenger ulike nøkler for hver dør. Dermed reduseres risikoen for sikkerhetsbrudd knyttet til administrasjonen av mange brukernavn og passord (en vanlig strategi for administrasjon av mange brukernavn og passord er å skrive dem ned på lapper som er lett tilgjengelige for brukeren selv – og for uvedkommende).[39]

Likevel er det visse sikkerhetsutfordringer assosiert med Feide. For når én nøkkel åpner mange dører, er sårbarheten åpenbar: faller nøkkelen i feil hender, kan uvedkommende få tilgang til alt som ligger skjult bak hver eneste dør. Et lite feilgrep – du mister ditt brukernavn og passord – kan derfor få store konsekvenser (hvis det er én nøkkel til hver dør, vil konsekvensene av at én av dem faller i feil hender trolig være langt mindre). I en skolesammenheng kan denne sårbarheten få problematiske konsekvenser. For det første, og som diskutert i forbindelse med digitale læringsplattformer, kan dette skje hvis elever får tilgang til lærerens brukernavn og passord. Da kan de for eksempel få tilgang til lærerens private mapper og alle elevopplysningene som læreren har registrert og lagret der. For det andre kan noe tilsvarende skje hvis læreren forlater sin PC i klasserommet uten å logge seg ut (og samtidig glemmer å benytte skjermlåsen). Dette sikkerhetsbruddet kan få særlig alvorlige konsekvenser hvis skolen også benytter Feide til innlogging på det skoleadministrative systemet. I et slikt scenario vil elevene ikke bare ha tilgang til elevinformasjon på den digitale læringsplattformen, men de kan også få tilgang til og mulighet til å endre karakterer, fraværsstatistikk og anmerkninger i det skoleadministrative systemet. Denne sikkerhetshendelsen oppstår altså fordi når du først er logget inn på én Feide-tjeneste får du tilgang til de andre tjenestene som brukes ved

37 Feide vurderes til å befinne seg på sikkerhetsnivå to i henhold til Fornyings- og administrasjonsdepartementets gradering av sikkerhetsnivåer (se *Rammeverk for autentisering og avviselighet i elektronisk kommunikasjon med og i offentlig sektor* (2008)). Det betyr bl.a. at Feide ikke skal brukes som innloggingsløsning for IT-systemer hvor sensitive personopplysninger behandles.

38 Sikker innlogging innebærer at to typer feil unngås: falsk positiv (noen som ikke har rett til å bruke systemet eller tjenesten får likevel tilgang) og falsk negativ (noen som har rett til å bruke systemet eller tjenesten får likevel ikke tilgang).

39 Se Thomas Olsen (2010): *Personvernøkende identitetsforvaltning*. PhD-avhandling, Det juridiske fakultetet, Universitetet i Oslo.

skolen uten å oppgi brukernavn og passord på nytt. Brukernavn og passord trenger derfor ikke å falle i feil hender for at sikkerheten til personopplysningene kompromitteres.

Etter som sikkerheten i Feide vurderes å være for dårlig til å anvendes i IT-systemer som inneholder sensitive personopplysninger (se fotnote 36 ovenfor), er en mulig sikkerhetshendelse at dette ignoreres av skolen/skoleeier. Det typiske scenarioet er at skolen/skoleeier ikke har gjennomført risikovurderinger av Feide for identitetsforvaltningstjenesten innføres. Dermed tilbys Feide-innlogging også i IT-systemer hvor det er stor sannsynlighet for at sensitive personopplysninger registreres. I så fall, og som vi har sett ovenfor, skal det ikke så mye til for at konfidensialiteten eller integriteten til opplysningene blir brutt (uvedkommende får tilgang til og kan endre sensitive personopplysninger).

Hjemmesider

En e-forvaltningstjeneste som de aller fleste skolene i Norge nå har, er hjemmesider. Hvordan skolene anvender sine hjemmesider kan være noe ulikt, men de presenterer i stor grad informasjon av generell og statisk karakter. I tillegg publiseres nyhetssaker med ujevne mellomrom. Det er vanligvis rektor, webansvarlig ved skolen eller utvalgte lærere som publiserer og oppdaterer informasjon på hjemmesiden.

Det er ikke så vanlig at hjemmesidene benyttes til elevaktivitet fordi mye av dette arbeidet foregår på de digitale læringsplattformene. På skolenes hjemmesider eksponeres det derfor lite personopplysninger, men enkelte grunndata om ansatte vil man ofte finne her (navn, stilling og telefonnummer). Dette innebærer at risikoen for brudd på personopplysningenes sikkerhet er relativt liten i forhold til hjemmesider. Den viktigste utfordringen er selvsagt muligheten for publisering av opplysninger – enten i form av tekst, bilder, video eller lyd – som representerer uønsket (og uautorisert) eksponering av personopplysninger. Hvis skolen for eksempel offentliggjør bilder av elever som lever på skjermet adresse, kan dette i verste fall få alvorlige konsekvenser (tap av liv eller helse). Og selv om sannsynligheten for at «det verst tenkelige» inntreffer vurderes som liten (for eksempel ved at bildene raskt ble fjernet fra hjemmesiden), kan vissheten om at opplysningene er blitt offentliggjort være en stor belastning for de som blir utsatt for denne typen konfidensialitetsbrudd.

En annen sikkerhetsrisiko er at bilder av elever eller ansatte som offentliggjøres på skolens hjemmeside kopieres, manipuleres og publiseres i andre sammenhenger. Bildemanipulering representerer et brudd på personopplysningenes integritet (uautorisert endring), men det er lite som tyder på at dette er et utbredt problem i norsk skole.

Skytjenester

Bruken av såkalte skytjenester synes ikke å være veldig omfattende i norsk skole per dags dato, men interessen for denne typen tjenester virker å være økende. Google Docs, Gmail, Live@Edu, Facebook eller Dropbox kan alle sies å være eksempler på skytjenester, og disse er allerede i bruk ved en del grunn- og videregående skoler.[40]

Et vesentlig poeng med skytjenester er at lærere og elever skal kunne skrive, dele, kommentere og rette i dokumenter som ikke ligger lagret på det lokale nettverket, men hos én eller flere eksterne leverandører (Google, Microsoft, Facebook, osv.). Det betyr bl.a. at brukergenererte data – arbeidsdokumenter og ferdige elevarbeider – ikke befinner seg i skolens eller skoleeiers varetekt, men overlates til eksterne aktører (gjerne multinasjonale selskaper som tilbyr både programvare, prosessorkraft, lagringskapasitet, osv.). Verken skolen eller skoleeier trenger derfor å vite hvilke land personopplysningene overføres til og oppbevares i.

Skytjenester reiser en rekke problemstillinger i forhold til personvern og informasjonssikkerhet. Det grunnleggende spørsmålet er hvilken kontroll skolen/skoleeier har med de opplysningene som overlates til leverandørene av skytjenester. Det finnes ikke et enkelt svar på dette spørsmålet, men svarene vil trolig varierer en del avhengig av hvordan skytjenestene er organisert (privat sky, offentlig sky, hybrid sky, osv.).[41] Og siden skolene i Norge har relativt begrenset erfaring med bruken av skytjenester, blir det ikke lett å vite hvilke konkrete personvern- og sikkerhetsutfordringer som bruken av skytjenestene innebærer. Men med bakgrunn i reglene i personopplysningsloven med forskrift, kan vi likevel antyde enkelte spørsmål som skolen/skoleeier bør avklare før tjenestene tas i bruk:

- Kan skolen/skoleeier ivareta den femte basisferdigheten – digital kompetanse – på en like god måte uten å bruke skytjenester?
- Kan skoleeier få leverandøren av skytjenesten til å undertegne en databehandleravtale og har skoleeier mulighet til å sjekke at tjenesteleverandøren følger opp vilkårene i avtalen?
- Er innholdet i tjenesteleverandørens personvernerklæring forståelig?
- Kan tjenesteleverandøren endre innholdet i personvernerklæringen etter eget forgodtbefinnende?

40 Skytjenester defineres av det amerikanske standardiseringsorganet NIST som «(…) en modell for nettbasert tilgang til mengder av konfigurerbare, delte dataressurser som raskt kan allokeres og avgis etter behov, med minimal administrativ innsats eller involvering av kunden» (se http://csrc.nist.gov/groups/SNS/cloud-computing/cloud-def-v15.doc).

41 Se for eksempel Senter for IKT I utdanningen (2010): *Bak skyen er himmelen alltid blå? En innføring i Cloud Computing for skoleeiere*.

- Kan skolen/skoleeier påvirke hvor i verden tjenesteleverandøren oppbevarer skolens personopplysninger?
- Hvilken personvernlovgivning gjelder i de landene hvor tjenesteleverandøren oppbevarer skolens personopplysninger?
- Kan skolen/skoleeier vite om tjenesteleverandøren vil utlevere skolens personopplysninger til andre sky-aktører?
- Kan skolen/skoleeier vite at personopplysningene vil være tilgjengelige når skolen har behov for dem?
- Hva skjer med personopplysningene hvis tjenesteleverandøren går konkurs eller blir oppkjøpt av en konkurrerende virksomhet?
- Hvordan kan skolen/skoleeier vite at tjenesteleverandøren ikke oppbevarer kopier av personopplysninger som slettes fra leverandørens lagringsområde?

Hvordan tjenesteleverandøren besvarer disse spørsmålene, kan være avgjørende for om skolen/skoleeier velger å bruke den aktuelle skytjenesten (forutsatt, selvsagt, at spørsmålene faktisk stilles). Prinsippet er at jo større kontroll tjenesteleverandørene gir skolen/skoleeier over personopplysningene, desto tryggere kan skolen/skoleeieren være på at det er mulig å overholde reglene om informasjonssikkerhet (og motsatt). Men at selskaper som Google, Facebook eller Twitter skulle ønske å gi skolen/skoleeiere stor grad av kontroll over personopplysningene fremstår (i alle fall per i dag) som relativt usikkert. For mens skolene ser på seg selv som tjenesteleverandørenes kunder, er det trolig at tjenesteleverandørene ser på skolene som sitt produkt: skytjenester genererer økonomiske verdier når de innhøster personopplysninger fra skolene som senere kan benyttes til formål bestemt av tjenesteleverandørene selv (for eksempel til individtilpasset markedsføring). I den grad dette er tilfelle, vil tjenesteleverandørene trolig være lite interessert i at skolen/skoleeier påvirker vilkårene for hvordan personopplysningene håndteres.

Ikke-teknologiske faktorer

Så langt har fremstillingen fokusert på hvordan den teknologiske utviklingen i skolen – bruk av IKT – fører til nye utfordringer både når det gjelder å sikre personopplysninger (slik at personvernkrenkelser unngås) og i forhold til etterlevelse av de rettslige kravene til informasjonssikkerhet. I den siste delen av artikkelen vil jeg peke på enkelte ikke-teknologiske faktorer og utviklingstrekk som også har betydning for informasjonssikkerhet og personvern i skolen. Som drøftelsen så langt har indikert, kan ikke den teknologiske utviklingen og de ikke-teknologiske faktorene diskuteres atskilt fra hverandre: analyser

av sikkerhetshendelser og regeletterlevelse må ta utgangspunkt i at tekniske sårbarheter, organisatoriske eller institusjonelle rammer (regler og prosedyrer, verdier og normer), sektorlovgivningen og individuell brukeratferd virker sammen. Det er derfor det samlede produktet av dette samvirke som avgjør sikkerhetstilstanden og regeletterlevelsen i skolen. Det er fire ikke-teknologiske faktorer som det er spesielt verdt å legge merke til i denne sammenheng.

For det første, og selv om den tidligere grunnskoleloven også inneholdt regler om individuelt tilrettelagt undervisning (§ 7.1) og spesialundervisning (§ 8), har prinsippet om individuell tilrettelegging blitt styrket og behovet for spesialundervisning økt i løpet av de siste årene (samtidig som begge deler er tydeligere rettighetsfestet i dagens opplæringslov).[42] Poenget med både individuell tilrettelegging og spesialundervisning er å gi et likeverdig opplæringstilbud til alle elever. Mange av de sikkerhetsutfordringene som er diskutert ovenfor – spesielt de som knytter seg til sikkerheten rundt sensitive eller sterkt personlige personopplysninger – må forstås mot denne bakgrunn. Den grunnleggende logikken som knytter sammen disse to faktorene – likeverdig opplæring (individuell tilrettelegging og spesialundervisning) og informasjonssikkerhet – kan oppsummeres på følgende måte:

- likeverdig opplæring forutsetter et individuelt differensiert opplæringstilbud,
- individuell differensiering forutsetter mer informasjon om den enkelte elev,
- mer informasjon innebærer elektronisk behandling av flere personopplysninger (både med hensyn til typer opplysninger og detaljeringsgrad),
- økende behandling av personopplysninger gjør det mer utfordrende å ivareta sikkerheten og å etterleve reglene om informasjonssikkerhet.

Dette viser at informasjonssikkerhet og personvern går til kjernen av, og er uløselig knyttet til, hvordan skolen utøver sine tradisjonelle hovedoppgaver. Men samtidig kan denne nære koblingen føre til at sikkerhet og personvern ikke figurerer på pedagogenes oppmerksomhetshorisont, spesielt når beskjeden fra nasjonale skolemyndigheter (og fra resultatene i internasjonale kunnskapstester) er at skolene ikke ivaretar sine tradisjonelle hovedoppgaver godt nok.

For det andre er skolen en offentlig institusjon som preges av åpenhet, høyt aktivitetsnivå og komplekse og tette sosiale relasjoner (elev-lærer, elev-elev, lærer-lærer, lærer-foreldre, osv.). Åpenheten kommer bl.a. til uttrykk gjennom nærskoleprinsippet (skolen skal ligge nært hjemmet), at opplæringen skjer i

42 Dette gjelder i særlig grad retten til spesialundervisning (eller i det minste retten til å kreve utredning av behovet for spesialundervisning). Se opplæringsloven kapittel fem og Utdanningsdirektoratets veileder: *Spesialundervisning – veileder til opplæringsloven om spesialpedagogisk hjelp og spesialundervisning*.

samarbeid med hjemmet, skolens omfattende rådsstruktur (spesielt i grunnskolen) og utstrakt samarbeid med andre nærmiljøaktører (for eksempel lokale lag, foreninger og næringsliv). Men skolens «kultur for åpenhet» kan til en viss grad stå i motsetning til en personvern- og sikkerhetstenkning (og praksis) som betinger at åpenheten blir mer styrt og kontrollert enn hva som tidligere har og fortsatt synes å være tilfelle. I tillegg kjennetegnes skolesamfunnet av til dels hektisk aktivitet (både i og utenfor klasserommet) som involverer mange aktører og hvor den fysiske (og emosjonelle) avstanden mellom de ulike aktørene er relativt liten.[43] Videre skiftes store deler av brukermassen ut hvert år: mange elever går ut av skolen og mange nye kommer til. Komplekse relasjoner, mange aktører, stor utskifting og mylderet av aktivitet, kan bidra til at det blir vanskelig for skolen å etablere den styringen, kontrollen og forutsigbarheten i sin elektroniske behandling av personopplysninger som reglene om informasjonssikkerhet forutsetter.

For det tredje kan det hevdes at kulturen i skolen preges av en ikke ubetydelig grad av individuell autonomi i hvordan lærergjerningen utøves (lærerautonomien er trolig større på ungdomstrinnet og i videregående opplæring enn på barnetrinnet). Lærerautonomien er intimt koblet til den metodefriheten som lenge har kjennetegnet planleggingen og gjennomføringen av undervisningen, det vil si lærerens individuelle rett til å bestemme hvilke pedagogiske virkemidler som han/hun ønsker å benytte for å oppfylle de faglige målene som lov- og læreplanverket pålegger skolen å ivareta. Samtidig kan det synes som om autonomien og metodefriheten påvirker hvordan skoleledere og lærere behandler personopplysninger, spesielt muligheten for at hver enkelt leder eller lærer utvikler sin private behandlingspraksis. Det kan for eksempel gi seg utslag i at minnepenner, datamaskiner, private mapper, fellesområder, osv. – og de personopplysningene som befinner seg her – ikke alltid håndteres i henhold til interne regler om informasjonssikkerhet: sensitive personopplysninger lagres hvor de ikke skal lagres (digital læringsplattform eller bærbar PC), sterkt

43 Det fører bl.a. til at improvisasjon – å løse praktiske problemer under stort tidspress – er et fenomen som ikke er ukjent i skolehverdagen. Men samtidig kan improvisasjon komme i konflikt med hensynet til informasjonssikkerheten. Det kan for eksempel skje hvis læreren oppdager at en av elevene ikke har en fungerende PC. Dette er et problem som læreren må løse der og da – og med hjelp av de virkemidler som han eller hun har for hånden (læreren har ikke tid til å vente på at IT-personell «fikser» elevens datamaskin) – hvis undervisningen skal kunne gjennomføres som planlagt. Derfor låner læreren ut sin bærbare maskin og eleven får tilgang til alle dokumenter og personopplysninger som er lagret på PC-en. I tillegg kan liten fysisk avstand mellom aktørene i skolesamfunnet føre til sikkerhetsutfordringer, for eksempel at individuelle opplæringsplaner blir liggende på printere som mange (både andre ansatte og elever) har tilgang til.

personlige opplysninger fraktes ureglementert mellom ulike destinasjoner (på ukryptert minnepenn), osv.

Denne typen privat behandlingspraksis kan selvsagt ikke bare (og heller ikke først og fremst) forklares med individuell autonomi og metodefrihet. Hva som oppfattes som lettvint og hensiktsmessig i en travel arbeidshverdag, sammen med liten kjennskap til lokale sikkerhetsrutiner (i den grad slike eksisterer) og at informasjonssikkerhet ikke er en del av pedagogers kjernekompetanse, er nok de viktigste forklaringsfaktorene. Men dette endrer likevel ikke det grunnleggende poenget, nemlig at den individuelle autonomien og metodefriheten er sider ved lærernes profesjonsidentitet som ikke alltid kommer godt overens med den byråkratiske rutinemessigheten som informasjonssikkerhetsarbeidet forutsetter (og som reglene i personopplysningsloven og forskriften krever).

For det fjerde kombinasjonen av at (i) skolen har begrenset erfaring med bruk av IKT og (ii) innføringen av datamaskiner, programvare og elektroniske nettverk har skjedd i løpet av en forholdsvis kort tidsperiode.[44] Denne kombinasjonen av omstendigheter – begrenset erfaring med og rakt utrullering av IKT – reiser spørsmålet om skolen har blitt tilført (eller har sørget for å skaffe seg) den brukerkompetansen som er nødvendig for å håndtere en ny og digital skolehverdag?[45] Manglende kompetanse i pedagogisk bruk av IKT, er én utfordring. Manglende kompetanse i det som skjer rundt den pedagogiske bruken av IKT, og hvordan IKT både endrer betingelsene for skolens administrative arbeid og samarbeidet med hjemmet, er en annen. I den grad det er slik at mange skoleledere og lærere sliter med å vite hvordan IKT kan utnyttes i læringsarbeidet, er det ikke overraskende at de også har vansker med å oppfylle kravene til informasjonssikkerhet og personvern som følger av lovverket. Denne typen regelverkskompetanse figurerer neppe på øverste halvdel av skoleledere og læreres liste over etterutdanningsønsker.

Denne gjennomgangen av ikke-teknologiske faktorer mer enn indikerer at skolen ikke lever av informasjonssikkerhet og personvern alene, men at skolen også ivaretar andre og viktige verdier, spesielt likebehandling, åpenhet, deltakelse, involvering, individuell autonomi og metodefrihet. I den grad hensynet til informasjonssikkerhet og personvern kan komme i strid med disse verdiene, er det ikke gitt hvem som skal gå seirende ut av striden. Utfordringen slik den avtegner seg i dagens skole, er å vite når informasjonssikkerhet og personvern skal prioriteres og når andre verdier og hensyn skal ha forrang.

44 Se kartlegginger av IKT-tilstanden i skolen, spesielt ITU Monitor 2005, 2007 og 2009.
45 Se for eksempel *Rapport fra tidsbruksutvalget*, 15. desember 2009.

Avslutning

Den norske skolen er i løpet av noen ganske få år blitt en viktig e-forvaltningsinstitusjon: diktafoner, filmfremvisere og skrivemaskiner er skiftet ut med bærbare PC-er, digitale læringsplattformer og Internett. Men sammen med alt det digitale, er det kommet noe annet med på lasset – nye utfordringer og regelverk som skolen plikter å forholde seg til. Dette gjelder i særlig grad (men ikke bare) kravene som personopplysningsloven med forskrift stiller til skolen og skoleeiers sikring av personopplysninger. Skolen som e-forvaltningsinstitusjon står derfor ikke bare overfor en utfordring når det gjelder å lære elevene digital kompetanse (for eksempel hvordan de skal ivareta sin sikkerhet og personvern på Internett). Det dreier seg i minst like stor grad om hvilken kapasitet skolen har til å ivareta lovpålagte krav om sikkerheten og personvern i sin egen behandling av personopplysninger.

Det er bare noen av disse utfordringene som har vært gjenstand for drøftelse i denne artikkelen. Det finnes i tillegg andre IT-systemer og prosesser som ikke er diskutert her, men som det hefter betydelige sikkerhetsutfordringer ved (for eksempel prosessene rundt utredning av og vedtak om spesialundervisning, bekymringsmeldinger til barnevernet, osv.). Likevel peker fremstillingen på viktige og grunnleggende sikkerhetsproblemstillinger som skolen, ifølge regelverket, plikter å ta på alvor. De viktigste årsakene til at slike problemer oppstår er at:

- mange elektroniske hjelpemidler benyttes til mange ulike formål og behandler store mengder sensitive og ikke-sensitive personopplysninger,
- mange ulike aktørgrupper (ledere, lærere, administrativt ansatte, elever, foreldre, osv.) lever tett innpå hverandre og alle har krav på at deres personopplysninger blir forsvarlig sikret (også i forhold til hverandre),
- aktører utenfor skoleporten (systemleverandører, skytjenester, driftsoperatører, barnevernet, PP-tjenesten, osv.) er involvert i behandlingen av personopplysninger og det kan være vanskelig å vite hvordan de ivaretar sikkerheten,
- skolen har begrenset kunnskap om hvilke rettslige plikter som gjelder for sikring av personopplysninger og hvordan pliktene kan etterleves.

Dette peker i retning av følgende hovedkonklusjon: Sikring av personopplysninger i en skolesammenheng (og kanskje spesielt i grunnskolen) fremstår som en vanskelig oppgave. Den viktigste årsaken til dette synes å være kombinasjonen av at (i) et mangfold av IT-systemer møter (ii) en offentlig institusjon preget av tette og komplekse sosiale relasjoner hvor (iii) sikker elektronisk behandling av personopplysninger er en ny og relativt ukjent problemstilling.

DA AKSJEBREVENE FORSVANT[1]

Olav Torvund

1 Innledning

Det norske aksjemarkedet «tok av» på begynnelsen av 1980-tallet, kort tid etter at *Einar Førde* kom med sin uttalelse om at å stimulere det norske aksjemarkedet var som å bære havre til en død hest. Aksjeomsetningen økte fra 1,7 mrd NOK i 1982 til 31,8 mrd NOK i 1985. Obligasjonsomsetningen økte fra 5,8 mrd NOK i 1983 til 75,9 mrd NOK i 1985.

Det daværende systemet var ikke i stand til å håndtere denne økningen. Man lå til tider månedsvis på etterskudd med å sluttføre transaksjonene. Det var en reell frykt for at hele oppgjørssystemet skulle bryte sammen under vekten av den voldsomme veksten. Noe måtte gjøres og det hastet. Dette hastverket satte et sterkt preg på arbeidet.

Finansnæringen satte full fart forover. Det var viktig å få etablert systemet og få satt det i drift. Det ble nedsatt en arbeidsgruppe, som i praksis fungerte som en styringsgruppe. Arbeidsgruppens sekretariat var bemannet for å utrede de praktiske, tekniske og økonomiske sidene ved etablering av en datasentral som kunne utføre oppgavene. At det var nødvendig med lovendringer og ny lovgivning, kom som en overraskelse på den arbeidsgruppen som skulle utrede dette. Sekretariatet var ikke bemannet for å utrede disse spørsmålene.

Tilfeldigheter gjorde at jeg, som eneste jurist i sekretariatet, var blitt trukket inn i dette arbeidet. Slik kom det til at en helt nyutdannet med en viss innsikt i elektroniske transaksjoner, men uten noen selskapsrettslig kompetanse eller kunnskap om verdipapirmarkedet, omtrent på egen hånd kom til å skrive den juridiske utredningen og lovforslaget i løpet av fire og en halv måned. Dog skal det sies at daværende lovrådgiver i Justisdepartementets lovavdeling, *Gudmund Knudsen*, var en uunnværlig støtte på det selskapsrettslige området.

Dette var bakteppet for lovendringene som åpnet for et «papirløst» aksje- og obligasjonsmarked og for etableringen av Verdipapirsentralen (VPS). Det bør ikke komme som noen stor overraskelse at mange spørsmål ble oversett, at ikke alt ble forstått og at en del problemer ble bevisst «feid under teppet» for ikke å skape unødig diskusjon om forslagene.

---

1 Artikkelen er opprinnelig publisert i «Selskap, kontrakt, konkurs og rettskilder: festskrift til Mads Henry Andenæs 70 år». - Oslo: Gyldendal akademisk, 2010.

2 Hindringer som måtte ryddes av veien

De rettslige sider av en overgang til ny teknologi vil det vanligvis foregå i to trinn. Første må man rydde bort hindringer, regler som binder en til den teknologi man vil bort fra. Teknologi er ikke bare datamaskiner m.m. Penn, papir, protokoller, hengemapper og dokumenter er også teknologi, selv om vi ikke er vant til å tenke på denne måten. Det neste, og langt vanskeligere trinnet er å etablere et rettslig grunnlag og rammer for det nye. Grensen mellom de to trinnene er ikke skarp. Man kan trekke meg seg gamle regler inn i det nye som ikke er et direkte hindrer en i å ta det nye i bruk, men som gjør at nye muligheter ikke kan utnyttes effektivt.

I den dagjeldende aksjeloven var det et krav om at det skulle utstedes aksjebrev. Ved overdragelse skulle aksjebrevene sendes inn til selskapet. Overdragelsen skulle føres inn i aksjeboken og aksjebrevene skulle få en påtegning om at dette var gjort, alternativt skulle det utstedes nye aksjebrev til erververe. I praksis hadde man innført aksjesertifikater som omfattet et større antall aksjer. Dette kravet var den viktigste retteslige hindringen som måtte ryddes av veien for å få en nødvendig modernisering av oppgjørssystemene for aksjehandel: De fysiske aksjebrevene måtte bort, i alle fall for børsnoterte selskaper.

Aksjebrevene hadde begrenset rettslig betydning. Det var innførsel i selskapets aksjebok som bestemte forholdet til selskapet, ikke aksjebrevet. Men i forholdet mellom avhender og erverver, og i forholdet til kreditorer, panthavere og eventuelle andre tredjeparter gjaldt dokumentrettslige regler gjennom en henvisning til gjeldsbrevloven.

For obligasjoner var situasjonen en annen. Det var ikke noen krav om at det skulle utstedes gjeldsbrev. Noen kredittforetak hadde på dette tidspunkt allerede etablert sine egne dokumentløse obligasjonssystemer. Men tok man bort dokumentet brøt man også tilknytningen til gjeldsbrevlovens kapittel 2. Fordringene var fortsatt gyldige, men de var ikke lenger negotiable. Er det et område hvor det kan være et reelt behov for at pengekrav er negotiable, så er det i obligasjonsmarkedet.

3 Dokument- og registersystemer – noen grunnleggende forskjeller

I en tid med begrensede og langsomme kommunikasjonstjenester ga dokumentsystemer gode og fleksible løsninger. Dokumentet kunne gå fra hånd til hånd og omsettes uten at den som hadde utstedt dokumentet behøvde å bli involvert i transaksjonen. De rettslige løsninger kunne bygges på eiendomsretten til det fysiske dokumentet også når dokumentet var bærer av abstrakte rettsgoder. Legitimasjon, og dermed adgangen til å utøve den rett dokumentet er bærer av, er basert på ihendehavelse, eventuelt i kombinasjon

med navngivelse og transportpåtegninger i dokumentet. Rettighetsovergang og rettsvern representeres ved overlevering av den fysiske rettighetsbærer.

I et registersystem er det ingen fysisk gjenstand som kan has i hende og eies. Legitimasjon kan ikke bygges på ihendehavelse. Man eier ikke en opplysning i et register slik at eiendomsrett til rettighetsbæreren ikke kan være grunnlaget for regler om rettighetsovergang m.m. Dette må knyttes til innførsler i registeret. Alle rettsendringer må registreres. All informasjon om transaksjoner må sendes til registret og en registreringsbekreftelse må sendes tilbake til partene i transaksjonen. Man er avhengig av rask kommunikasjon om dette skal fungere i et marked med stort transaksjonsvolum. Derfor har disse systemer tradisjonelt vært forbeholdt formuesgoder med høy verdi og lavt transaksjonsvolum.

Datasystemer og datakommunikasjon har gjort at kommunikasjon mot registeret kan skje raskt, mens transport og håndtering av papir blir den største flaskehalsen.

Det gamle aksjesystemet var en hybrid mellom et registersystem og et dokumentsystem. Man hadde aksjebrev, samtidig som alle overdragelser skulle registreres i aksjeboken. Denne løsningen kombinerte ulempene ved begge systemer.

Når man skal etablere en registerbasert løsning kan man velge en av to hovedmodeller: Et register føres hos en av partene i rettsforholdet, eller hos en uavhengig tredjepart. Aksjeboken ble ført hos selskapet, selv om dette for børsnoterte selskaper i praksis ble utført av aksjonærservice i de større bankene. Denne løsningen er beholdt for aksjeselskaper, se asl § 4-5. Det er også denne løsningen man får om prinsippet i gbl § 29 skaleres opp fra enkelttransaksjoner til et transaksjonssystem. Kredittforetakenes egne systemer før VPS var basert på dette. Det er også denne løsningen man har valgt for livsforsikring, se FAL § 17-1. Bankenes kontosystemer kan også ses på som et registersystem basert på denne modellen. En slik løsning må forutsette at man har den nødvendige tillit til den som registrerer opplysningene, herunder at denne ikke har noen betydelig egeninteresse i de transaksjoner som foretas.

Tredjepartsløsninger er velkjent fra bl.a. tinglysingen. Noen av fordelene med en nøytral registreringsenhet er ganske åpenbare: Registerenheten er uavhengig av partene. Det er dette som er valgt for verdipapirregistre, og for allmennaksjeselskaper kreves registrering i et slikt register, se aasl § 4-4.

Når systemet skal betjene et marked vil sentraliserte løsninger være en fordel, hvilket ytterligere taler for en tredjepartsløsning. Aktørene i markedet, i praksis meglerapparatet, behøver ikke forholde seg til et stort antall registre med ulike løsninger. VPS ble opprinnelig gitt monopol på å være verdipapirregister. Dette ble endret ved lov om verdipapirregistre i 2002. Men selv om det da ble åpnet for etablering av flere registre og konkurranse, har vi sett en

ytterligere sentralisering ved at VPS i 2007 ble fusjonert inn i samme konsern som Oslo Børs.

Et dokumentsystem er åpent. Den som har dokumentet kan levere dette til hvem som helst, på samme måte som vi kan betale til hvem som helst med kontanter. Et registersystem vil være lukket. Det kan ha mange eller få aksesspunkter, og dermed fremstå som mer eller mindre åpent. De to banknettverkene Visa og MasterCard fremstår som ganske åpne fordi det er så mange deltakere. Men alle deltakere må ha en avtale med systemet og tilfredsstille de krav som stilles for den aktuelle rollen. Den som skal gjennomføre en transaksjon vil alltid måtte gå via en «portvakt».

Når man er avhengig av å få tilgang til en lukket infrastruktur for å kunne delta i et marked gir dette konkurranserettslige utfordringer som vi her ikke skal gå inn på. Det gir også utfordringer i forhold til å betjene et internasjonalt marked. Hvis man ønsker utenlandske investorer er det ikke hensiktsmessig å kreve at alle som ønsker å kjøpe aksjer i norske selskaper først må knytte seg til en norsk infrastruktur. Man har derfor måttet akseptere forvalterregistrering hvor én aktør registrer aksjer på vegne av sine kunder. Myndighetene har gjerne vært skeptiske til slike løsninger, men man har i praksis måttet akseptere dem. Det ble først åpnet for forvalterregistrering av utenlandske aksjonærer i aasl § 4-10, i utgangspunktet bare for aksjer notert på utenlandsk børs (men med dispensasjonsadgang). Men ved den nye verdipapirregisterloven av 2002 ble det generelt åpnet opp for slik registrering i § 6-3.[2] Antagelig var dette en ganske utbredt praksis også før det ble tillatt å registrere eierskap på denne måten.

4 Markedstransaksjoner og rettsvernsakter

I våre tradisjonelle registreringssystemer har transaksjonen blitt registrert først etter at den har blitt gjennomført utenfor systemet. Det er den gjennomførte transaksjon som tinglyses og det var den avsluttede avtale om aksjekjøp som ledet til registrering i aksjeboken. I dagens verdipapirregistre kombineres disse funksjoner i ett system. De utfordringer dette gir var det nok ingen som forsto da den første loven ble vedtatt i 1985. Erkjennelsen sank inn etter noe tid, og da jeg skrev en kommentar til lov om VPS i 1987 hadde i alle fall jeg innsett at dette ikke hang sammen. Men jeg hadde nok bare sett problemet uten å finne løsningen. Etter å ha drøftet en rekke mulige forståelser av prioritetsregelen i 1985-lovens § 5-1, summerte jeg det opp slik:[3]

2 Se nærmere om dette i Ot.prp. nr. 39 (2001-2002) kap. 9.
3 Torvund: Lov om verdipapirsentral med kommentarer, TANO 1987, s. 261.

De skisserte løsningene bygger på et særdeles svakt rettskildemessig fundament. Problemene omkring prioritet mellom rettsstiftelser i fondsaktiver registrert i VPS er ikke tilfredsstillende løst i loven og er bare i liten grad drøftet i forarbeidene. Reglene er uklare, og slutninger trukket på bakgrunn av disse blir derfor usikre. Det er heller ikke mulig å finne klare analogier fra andre rettsområder. Det hele må derfor avgjøres ut fra en vurdering av de reelle hensyn. Men heller ikke på dette grunnlag er det klar overvekt for en bestemt løsning. Og alle løsninger som det er praktisk mulig å gjennomføre på en hensiktsmessig måte vil i noen tilfelle være i strid med lovens ordlyd.

Under arbeidet fram mot den nye loven fra 2002 var dette også noe som voldte mye hodebry og heller ikke denne gangen klarte man å få et godt grep om dette.[4]

Det som registreres inn i systemet fra markedet er uoppgjorte transaksjoner. Det registreres et kjøp og et salg. Ytelsen er generisk bestemt. Kjøper og selger handler via megler og kjenner vanligvis ikke til hverandre. Transaksjonene matches i systemet og synkroniseres mot betalingen. Inntil transaksjonen er gjort opp vil det bare være uoppfylte fordringer som er registrert i systemet. Det som skal leveres er ikke individualisert. Noen egentlig individualisering skjer ikke, bare en form for kvasiindividualisering ved at man kan vise til de finansielle instrumenter som i øyeblikket er registrert på en konto. Kjøper vet ikke hvem som skal levere og ingen levering har funnet sted. Den som har en uoppfylt fordring vil ikke ha noen form for rettsvern mot avhenders kreditorer.

Det gir heller ikke særlig mening å snakke om rettsvern mot konkurrerende erverver ved levering av ikke individualiserte genusytelser. Dersom levering ikke skjer vil man ha et regulært mislighold, og i praksis vil det være megler og ikke den egentlige selger som må sørge for oppfyllelse overfor kjøper.

De tradisjonelle rettighetsregistrene er åpne. De skal sørge for publisitet og notoritet. Et verdipapirregister er ikke åpent. Utgangspunktet er tvert imot at opplysningene er underlagt taushetsplikt etter § 8-1, kombinert med særskilte innsynsregler i § 8-2. I tillegg kommer regelen om innsyn i aksjeeierregisteret etter aasl § 4-5.

Godtroerverv og etablering av rettsvern bygger på den grunnfortutsetning avhender er legitimert. Avhender skal ha et ytre skinn av rett. Et taushetsbelagt register skaper ikke noe slikt ytre skinn av rett for avhender. Og om det kunne ha gjort det, ville det likevel ikke hatt noen betydning så lenge erverver ikke

4 Det er ganske omfattende drøftelser av dette i NOU 2000: 10 kap 18, særlig 18.3.3, og i Ot.prp. nr. 39 (2001-2002) kap 11 under overskriften *Rettsvirkninger av registrering*.

vet hvem avhender er. Rådighet, eller manglende sådan, viser seg først ved levering.

5 Avslutning

Det har vært brukt mye energi på å finne rettslige løsninger som kan kombinere markedssystemet og rettighetssystemet. I 1985 vedtok man egne regler om hvilke innsigelser som kunne gjøres gjeldende og hvilke som ikke kunne gjøres gjeldende. I 2002-loven har man beholdt en egen bestemmelse for hjemmelskonflikter, mens man har gått tilbake til en henvisning til gbl §§ 15-17 når det gjelder innsigelser fra det underliggende forhold.

Skjæringspunktet for når rettsvirkningene inntrer er ikke klart angitt. I 1985-loven het det at rettsstiftelser registrert samme dag hadde lik prioritet, en regel som det i praksis var umulig å følge. Skulle en kollisjon oppstå ville man måtte la en vinne rett og den andre måtte ha blitt avspist med erstatning. Da dagens lov ble gitt i 2002 hadde man sett problemet, men man kan ikke si at det er løst. I § 7-1 siste ledd heter det:

> *Rettighetsregisteret skal fastsette regler for når en rettighet er registrert. Reglene skal godkjennes av departementet.*

Et så viktig spørsmål som når rettsvirkninger i forhold til tredjepart inntrer skal bestemmes i regler som det enkelte rettighetsregister selv fastsetter. Dette er i dag regulert i VPS forretningsvilkår, avsnitt 7.[5]

Det kan sies mye om disse reglene, langt mer enn plassen her tillater. Løsningen fremstår ikke som god. Men likevel har systemet vært i virksomhet i mer enn 20 år uten at det har oppstått alvorlige problemer. Det spørsmål som da presser seg på er om denne reguleringen betyr så lite at selv alvorlige svakheter i den ikke får noen praktisk betydning. Jeg har kommet til den konklusjon at reguleringen på dette punkt faktisk betyr så lite.

I et registersystem hvor man håndterer abstrakte rettsgoder som ikke har noen materiell eksistens utenfor registeret vil man ikke få situasjoner hvor det er konflikt mellom det faktiske og det rettslige. Det er i spenningen mellom det faktiske og det rettslige vi har behov for regler om omsetningskollisjoner, om rettsvern osv. Den som ikke har rettslig rådighet over en konto i et verdipapirregister vil heller ikke ha noen faktiske muligheter til å råde over de verdier som innestående på denne kontoen representerer. Levering og registrering faller sammen og spørsmålet om rettsvern m.m. har ikke større betydning enn for

5 http://www.vps.no/public/content/download/1227/5482/file/Forretningsvilkaar.pdf

andre genusytelser. Man kan riktignok inngå avtaler som man i ettertid ikke kan oppfylle. Men da har man et regulært mislighold og kjøper må fremme krav på det grunnlag, ikke lete etter rettsvern til noe selger ikke disponerer over.

Arbeidet med etablering av et lovverk for et «papirløst» verdipapirmarked er et eksempel på en feil som har blitt gjentatt mange ganger når man går fra et system til et annet og skal utvikle regler for den nye virkeligheten. Man legger et stort arbeid i å finne løsninger for å kunne overføre de velkjente rettslige prinsippene til en ny virkelighet. Men man glemmer å stille det grunnleggende spørsmålet: Behøver vi å ta med oss alle de gamle prinsippene når vi forlater de gamle løsningene? For verdipapirregistre burde konklusjonen ha blitt nei.

THE LAWYER IN 2020[1]

Tobias Mahler

How will lawyers work in the year 2020? From the perspective of the year 2010, the future is necessarily unknown and uncertain. Without a time machine we cannot make solid predictions about what will be. Yet, this does not necessarily mean that it is impossible to say anything about the future. A weather forecast is roughly based on data about the present and an understanding of how similar situations have developed in the past. To some degree, the future of lawyers can be discussed in similar terms of a prognosis, focusing on the change we can reasonably expect within ten years. By understanding the lawyer of 2010 within the historical context and current technological and social developments we may develop some initial hypotheses about the future roles of lawyers.

In addition, we may also discuss the future as something that we can shape and form, at least to some degree. In this second and complementary perspective, we may ask how the role of lawyers ought to be within ten years. How could the provision of legal advice be improved? Can it be made more affordable? Should lawyers become more proactive, and how could this be achieved?

In this context, I will speak of what lawyers do as «services» and I will address the market for such services. Admittedly, lawyers' roles in the legal system go much beyond what can be captured within the concepts of the market for services. However, for lawyers' clients, who seek and pay for legal advice, this is at least one relevant perspective. Alternative perspectives could and should be used to complement the perspective I take here. These could, for example, include the future participation of lawyers in society, for example their power in society, and their contribution to a legal system based on the rule of law. Regrettably, these and other possible angles on the roles of lawyers have to be omitted here.

I will cover the following aspects: First, I will introduce two historical perspectives that may shed some light on the probable future. Then, I will briefly present an initial outline of possible future roles of lawyers. I will subsequently continue to examine two of the reasons for why these roles are being suggested:

- A likely technological innovation and

1 This paper is based on the author's trial lecture for the PhD degree in law at the Faculty of Law, University of Oslo, 31st of August, 2010.

- A possible demand for other innovations regarding the roles of lawyers.

Historical perspectives on the future

The present and the proximate future can perhaps be understood in terms of a convergence of two transitional phases in human history;
- the path to an IT-based information society and
- the process of globalization.

I would therefore like to direct your attention to the following two timelines.

Capturing legal information and knowledge

The first of these developments can be illustrated based on four phases during which information was captured and communicated differently in human history.

Figure 1: Capturing and communciating legal information and knowledge

Oral speech clearly dominated initially, then came the era of script, then print and now we are moving into an era during which information is increasingly captured in IT systems. [2] This information substructure in society has clear implications on how legal information is captured and communicated. Each of the transitions implied fundamental changes in how lawyers worked. The best-known example of the culmination of the first transition from oral speech to script is the Hammurabi Code, written in Babylon around 1760 BC. What is preserved today is a large stone, on which the code was inscribed. This may not be very impressing from today's perspective, but it is an example of how a rudimentary information system ensured that legal information was communicated consistently to the population of Babylon.

2 See further R. E. Susskind, *The End of Lawyers? Rethinking the Nature of Legal Services* (Oxford: Oxford University Press, 2008), 29.

Figure 2: The Hammurabi stone[3]

As for the second transition from script to print, we know that this lead to an unprecedented improvement in terms of access to legal information. There was an immediate exponential growth in the number of available books in regions where the printing press had been introduced. On the other hand, the societal consequences thereof took much longer to materialize, so I would not be surprised if the same would be true today.

We are currently witnessing the third transition in this timeline. Let me illustrate this with a contract I received earlier this year per e-mail. This is a very nice example, because the IT system still resembles very much the working modes of the print age. The contract I received is a PDF scan of a text. Thus, when negotiating the wording I need to again type the respective sentence. This nicely exemplifies some of the struggles of the transformation, and also shows the potential for more effective and efficient working methods.

It is probably not controversial to predict that this transformation to an IT-based information and knowledge society will be one of the driving factors for change in the proximate ten years. However, we need to take a closer look at the last phase of this model, in order to discuss how the introduction of IT tools could lead to a change in how lawyers work.

Professor Susskind has introduced the following model in order to discuss what he calls the evolution of legal services.[4]

3 Source: BrokenSphere/Wikimedia Commons.
4 Susskind, *The End of Lawyers? Rethinking the Nature of Legal Services*, 29.

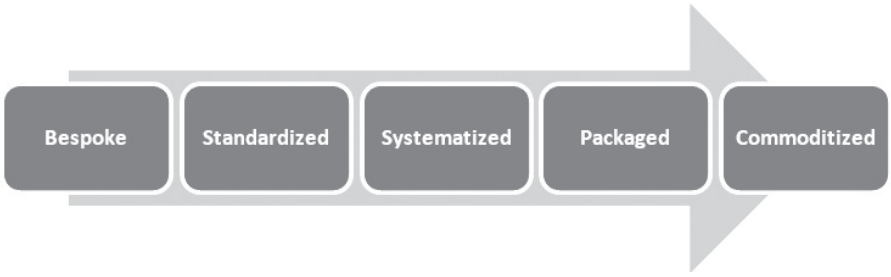


Figure 3: Evolution of legal services, based on the use of IT

Today, most lawyers focus on *bespoke* services. This is a traditional «handcrafted» consultative service, which is highly tailored for the specific needs of particular clients. Bespoke service also fits best with the business model of most law firms, if they are based on hourly billing. However, IT could be used to improve legal services, following a kind of evolutionary path. The basic idea in this model is that when elements of the bespoke service are being repeatedly offered, then they can to some degree, be *standardized* to avoid duplication. Standardization can both include the business-processes within which legal services are provided and the substance on which lawyers advise. When supported by dedicated IT tools, this could be called a *systematized* service. While the latter still focuses on the tasks within a law-firm, the next step makes *packaged* legal services available to clients. The most controversial step is arguably the last one. Susskind defines a legal commodity as an electronic legal package that is perceived as a commonplace, a raw material that can be sourced from one of various suppliers. The use of the term «*commodity*» implies that the legal service is being compared to barrels of oil and sacks of sugar.

The fact that the legal service can be sourced from a variety of providers implies that the service has become undifferentiated and that it is provided at a fairly low cost. For most lawyers, this seems like both an unattractive and perhaps unlikely future development. It is quite far away from both the teaching of our educational institutions and from the current business models of law-firms. Not least therefore, the path towards the right side of the model might seem unattractive for many lawyers. However, it does not seem unreasonable to assume that many clients of law firms would applaud a cheaper and more systematic service provision. Thus, there is likely to be a pull from the market towards the right side of the model.

I will examine more closely in a moment, in the context of specific technologies, whether the path to commoditization is technically possible and econo-

mically viable. However, before we do that, I would like to introduce a second timeline, which focuses on globalization.

Globalization

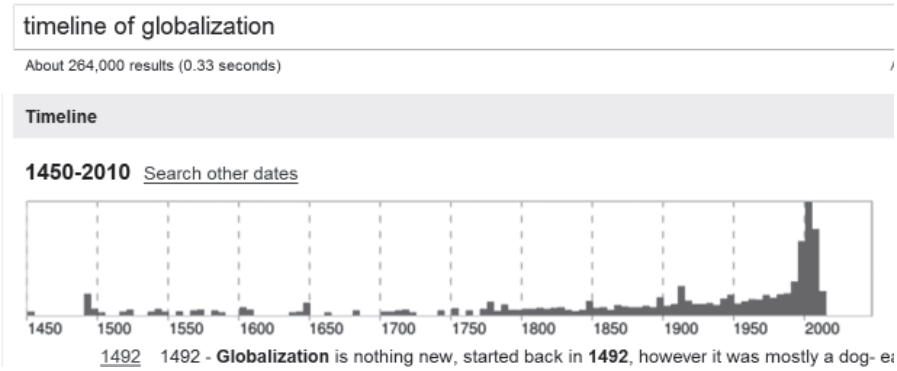


Figure 4: A timeline of globalization[5]

The timeline above illustrates the growing importance of globalization. This is a very real phenomenon we are witnessing in all areas, and particularly on the Internet. The timeline is also a case in point for what I said about IT tools. Google's timeline is clickable and seems to be auto-generated, based on available information on the web. Obviously, Google does not employ the world's best historians; they just use IT in a creative way to make sense of available information. A similar creative use of available legal information could make a considerable difference in the future. However, the example also shows some of the current limitations of technology. The software's understanding of historical dates is suboptimal, as it does not really make a distinction between the discovery of America in 1492 and a conference about globalization today. Thus, the peak around 2000 seems to indicate interest for globalization, rather than an actual increase in globalization. Concomitantly, there is no reason to believe that globalization is currently declining, despite the decreased frequency of occurrence of the word during the past few years. It is safe to anticipate that globalization will be at least as important in 2020 as it is today.

5 Source: Google.

Potential future roles of lawyers

Let us now turn towards the potential future roles of lawyers. The literature on this subject is surprisingly limited. The most concrete prediction about the future roles of lawyers was put forward by professor Susskind in his latest book.[6]

Susskind predicts that there will be a need for five roles of lawyers in the future. Notably, this perspective focuses primarily on lawyers who work as in-house counsel or in law-firms. Thus, other roles, such as the roles of lawyers working as judges or in public administration or academia do not seem to be the primary focus.

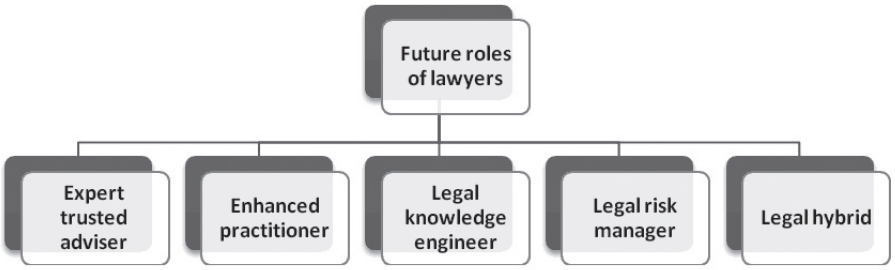


Figure 5: Susskind's prognosis[7]

The first type is fairly similar to the traditional role of a lawyer. The expert trusted advisor offers bespoke legal services, as mentioned above. Susskind envisages that there still will be a need for this legal role in the foreseeable future, but that bespoke services will be less competitive, if compared to alternative services that employ IT tools and standardization to provide a more efficient service.

The enhanced practitioner works further to the right of the above-introduced evolutionary path on Figure 3. This kind of lawyer supports the delivery of standardized, systematized and packaged legal service. However, when such tools are available and in use, then this lawyer may have to compete with other, less costly or differently qualified sources. For example, in-house lawyers may have to compete with contract managers.

6 Susskind, *The End of Lawyers? Rethinking the Nature of Legal Services*.
7 Based on ibid.

Susskind also predicts that there will be a need for an entirely new role: The legal knowledge engineer. These are professionals who design the systematized and packaged legal services. This will require a different competence from the one taught in law school, even though legal analysis is a necessary element of their work. In addition, such professionals will need to be able to handle the knowledge engineering perspective.

As you have seen, the first three roles are primarily described in terms of their use of IT. This does not seem to be true for the legal risk manager. This role focuses on the need for more proactive legal services. According to Susskind, many in-house lawyers feel that their role in the organization is the role of a legal risk manager. However, there is a lack of methods, tools and techniques or systems that might help clients to identify, quantify and control the legal risks they face. I will briefly expand on this role later.[8]

The fifth role is what professor Susskind calls a legal hybrid. Already today, many lawyers do not conceive themselves as primarily lawyers, but rather as management consultants, market experts, deal brokers, and so on. He anticipates that lawyers will continue to work in such hybrid roles, but that the need for rigorous education in the related disciplines will increase.

As mentioned, the first three roles are primarily defined based on their use of technology, while the ultimate two seem to primarily address other needs, related to, respectively, proactive and multi-disciplinary services. Therefore, this model might be slightly amended as follows.

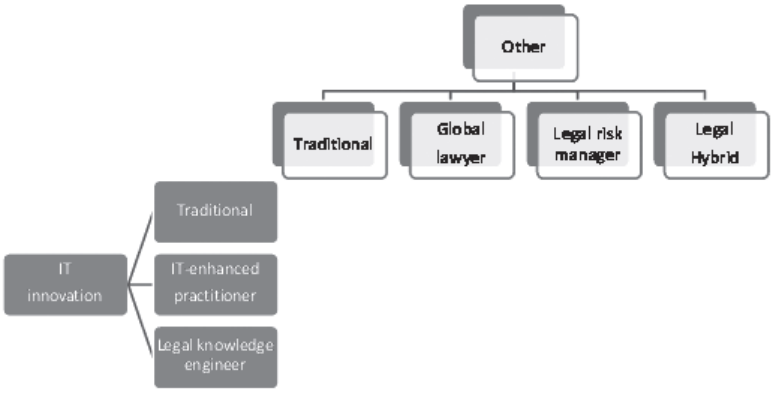


Figure 6: A possible modification of Susskind's prediction

8 See further Tobias Mahler, *Legal Risk Management: Developing and Evaluating Elements of a Method for Proactive Legal Analyses, With a Particular Focus on Contracts*, PhD dissertation, University of Oslo, 2010.

In this diagram I have attempted to distinguish between (i) changes that are primarily due to IT innovation and (ii) other possible changes in the roles of lawyers. This also allows us to include the global lawyer, which did not fit into the previous model.

In terms of the expected IT innovations, the model still distinguishes between three roles, which are only slightly renamed. The key difference to the previous model is that the above-shown «other» roles can be combined with different degrees of IT use. Thereby, for example, the IT-enhanced practitioner could work in a more traditional fashion, as a global lawyer, as a legal risk manager or as a legal hybrid. Thus, the diagram is changed form a one-dimensional model to a matrix. Obviously, this model could be even further extended both with additional roles, additional depth and further dimensions, but this cannot be done here.

In the following, I will examine first the possible changes in the roles of lawyers that follow from the introduction of new technology. Subsequently, I will briefly address the need for a global lawyer and a legal risk manager.

The impact of technology changes

I now turn to how the future development of IT might impact the role of the lawyer in 2020. Some examples of future IT-enabled approaches and tools are listed below in Table 1.[9]

Future approaches?	**Examples of tools**
Visualization	Legal wikis
Natural language processing	Automated document assembly
Embedded legal knowledge	Online legal guidance
	Integrated tools, e.g. for contract management

Table 1: Examples of IT-based approaches and tools

Let us first address some future approaches that could impact the roles of lawyers. *Visualization* is not necessarily new; many old law books are richly illustrated.[10] However, today visualization is increasingly used to simplify the communication of legal information. For example, the icon below is used by

9 For a detailed discussion of the impact of some of these technologies, see ibid.

10 Brunschwig C. Brunschwig, *Visualisierung Von Rechtsnormen Legal Design*, Zürcher Studien Zur Rechtsgeschichte 45 (Zürich: Schulthess, 2001).

Creative Commons to illustrate that certain content may not be re-used for commercial purposes.

Figure 7: Visual representation used by Creative Commons[11]

Natural language processing today sounds rather futuristic in the legal context. It aims at computer systems that analyze, attempt to understand, or produce human languages, such as English or Norwegian. Today, it is already possible to analyze legal texts in a variety of languages and to distinguish certain concepts, such as normative modalities (e.g., obligations and prohibitions).[12] Clearly, if and when the software really can approach something like an understanding of the law or the contract under analysis, this might lead to fundamental changes.

The notion of *embedded legal knowledge*[13] appears to be somewhat wider than, respectively, Lessig's notion of *code*[14] and Reidenberg's notion of *lex informatica*.[15] Examples include the following: Vehicles can already today have special locks to ensure that intoxicated drivers cannot drive them. And car sensors are currently learning to read traffic signs; in the future, some degree of traffic law compliance is likely to be embedded in our vehicles. This requires that the role of legal advice will be transformed, as its focus shifts towards the design and control of technology.

Another significant factor for the lawyer in 2020 is the support by dedicated *IT tools*. Wikipedia is well known and much used, and we are increasingly witnessing the development of *legal wikis*. Today, the information found there is not very impressing, but this might change in the future.

11 Source: creativecommons.org.

12 See, e.g., C. Biagioli, E. Francesconi, A. Passerini, S. Montemagni, C. Soria, «Automatic semantics extraction in law documents», *Proceedings of the 10th international conference on Artificial intelligence and law*, June 06-11, 2005, Bologna, Italy.

13 Susskind, *The End of Lawyers? Rethinking the Nature of Legal Services*, 141 et seq.

14 L. Lessig, *Code Version 2.0* (New York: Basic Books, 2006).

15 J. Reidenberg, «Lex Informatica: The Formulation of Information Policy Rules through Technology,» *Tex. L. Rev.* 76 (1997).

Automated document assembly systems can be used to generate legal documents, based on text template. Many such systems are already in use.

On-line legal guidance systems are web-based resources that contain knowledge of lawyers that is no longer accessed exclusively by consultation with human advisers. One example is the Norwegian Bar Association's website, where users may assess, for example, risks related to their marital status.

Figure 8: Risk test (online guidance system)[16]

The user answers a set of simple questions and the system provides some form of initial legal advice. Notably it is a computer, and not a lawyer, who provides the information. I have done the text myself. You may see that I received a number of red and yellow flags, which represent additional examples of visualization. When assessing the risk, this system disregards the rather important question whether I will in fact be separated. It just says that if there were a separation, then certain financial aspects would be difficult to calculate. Currently, online legal guidance often caters for what has been called the latent market: People who may not previously have had access to legal advice may now receive at least basic advice from an online system. However, this is by no means the only way of using online guiding systems.

A *contact management* system focuses on managing a contract lifecycle. It usually covers at least the drafting, review and negotiation of a contract. Currently available contract management systems are usually combinations of workflow tools and a centralized repository, but the tool can also help with performance monitoring. The aim for contract management is primarily to maximize efficiency and minimize risks in any contracts. A contract management system could initially improve the work of lawyers and their colleagues,

16 Source: advokatenhjelperdeg.no.

who today often are struggling with e-mail-based contact negotiations and contracts that float around in the organization. However, such tools may in the future offer semi-automatic checks of contracts and facilitate a structured assessment of risk. And it is an open question to what degree such management systems will need to be used by lawyers. Already today, the contract manager is an emerging role in many organizations, and these professionals are by no means only lawyers.[17]

Disruptive legal technology?

How will these possible technological changes impact the roles of lawyers and their clients? For the latter, the changes would appear to be primarily positive, because legal information becomes more accessible and affordable, even though there would seem to remain important areas for which legal information would have to be obtained from a lawyer.

Will lawyers also welcome these changes? In business literature there is a distinction between two distinct types of innovation, which is perhaps relevant here.[18] The first is *sustaining innovation*. For example, given our experiences so far, we may expect that we will have access to better and faster computers in 2020. Similarly, we might anticipate innovations to improve many aspects of legal services. I would see visualization as an example of sustaining innovation. A possible increase in visual communication by lawyers will not lead to significant changes, but a better communication with non-lawyers might at least count as a small step ahead.

This can be contrasted with what may be called *disruptive innovation*. The latter leads to a fundamental transformation of the market. For example, no matter what you do to improve the performance of CDs and DVDs, it is questionable whether they will be able to compete with a growing market for on-line music and films. Or, historically, no matter what one did to improve the hand-copying of books, there was no chance to beat the book-press. It has been claimed that some of the technologies I have mentioned, *inter alia*, could be disruptive for lawyers in the long run. The thesis is that these and other innovations may reduce the need for a traditional expert trusted adviser and increase the need for the other roles.[19]

17 On the role of contract managers see, e.g., the International Association for Contract and Commercial Management, IACCM, at iaccm.com.

18 C. M. Christensen, *The Innovator's Dilemma When New Technologies Cause Great Firms to Fail*, Rev. ed., The Management of Innovation and Change Series (Boston, Mass.: Harvard Business School Press, 2003).

19 Cf. Susskind, *The End of Lawyers? Rethinking the Nature of Legal Services*, 93 et seq.

Can we see disruptive legal technology at the horizon? Perhaps we should distinguish between different degrees of disruption. It does not seem entirely unlikely that certain elements of the market for bespoke legal services could be diminished, or at least decreased, by a widespread use of new technologies. When legal information is radically better available and offered in a more structured and cheaper manner, then some current business models may indeed partly fail in the future. For the lawyers' customers it may be less attractive to pay a lawyer by the hour than to use a combination of an effective IT-based service and lower-cost labour. Thus, in the long-term perspective, some degree of disruption cannot be excluded, although I am unsure about whether we will witness significant disruptions as early as 2020. Amongst the factors that contribute to uncertainty is that there are also developments towards increased complexity, which may slow down such disruptive effects, or even lead to opposite outcomes. At least in the short and medium term perspective, globalization seems to imply an increased complexity, with which lawyers have to deal.

I will now turn towards the global lawyer and the legal risk manager. Both of these roles are not induced by a technological change, but by other demands.

The global lawyer

The need for a global lawyer[20] can be exemplified with the following situation, which is not exaggerated. Some day earlier this year, a German lawyer in Norway receives the following e-mail from Brazil: –»… they reject the French conditions. Until when can you analyze the Argentinean ones?»

The role of a global lawyer is currently very difficult or impossible to fulfil for any individual. You may remember the old environmentalist slogan: «Think globally, act locally!» Usually, it seems, most of us lawyers do the opposite. Even though we sometimes *act globally*, we inevitably *think* primarily in *local* terms of the legal system in which we were educated. Based on our education and socialization, we become part of a particular legal culture. Regrettably, it is often difficult to get a sufficient understanding of the other legal systems and cultures. Law faculties across the world apply different strategies to create awareness and to strengthen language proficiency, but this does not solve all problems. Today, certain legal sources are available on the Internet, such as the

20 Regarding the notion of a global lawyer, cf. e.g., Global Sourcing and the Global Lawyer, *Georgetown Journal of International Law - Symposium 2007. To watch the archived webcast video of the panels or to download the audio in a «podcast» form, please visit: http://www.law.georgetown.edu/webcast/eventDetail.cfm?eventID=253.*

Argentinean civil code. So are a few introductory texts. However, the available texts do not necessarily help us to solve the problems of global business and local laws. Possibly, future legal information and knowledge systems might be able to furnish more of the know-how necessary to solve legal problems in a globalized world. However, no such solution is in sight today.

However, the example also indicates that is far from clear why a German lawyer in Norway should assist in a contract negotiation in Brazil. Global players will revisit and reconsider how they source legal tasks in a global economy. Thus, outsourcing of legal services may have a significant impact on the lawyer in 2020. To some lawyers this will appear as a dystopia. However, many clients will see this as an opportunity to reduce costs, and prospective legal service-providers in emerging economies will consider globalization as an unprecedented chance to compete within a new market.

The legal risk manager

Let us now turn towards another newcomer amongst the possible future roles of lawyers. Above it was already mentioned that the legal risk manager is already an emerging role of in-house counsels. Many clients prefer to anticipate and pre-empt legal problems, rather than needing to have to solve them when they occur. At least, this is what they say they prefer, before they consider the potential costs of pre-empting all legal problems. This is amongst the issues to be dealt with in legal risk management. Risk management, according to the ISO, refers to a set of coordinated activities to direct and control an organization with regard to risk. Legal risk management is described in detail in my PhD thesis, so I will only briefly mention some key aspects here.[21] The basic idea is that some risk management methods from other disciplines could be usefully adapted to the legal context. These would be the methods to be used by the legal risk manager.

The proposed aim of legal risk management is the adequate management of risk in the legal context. As conceived here, legal risk management is not confined to the management of legal risk, but also includes the management of other risk by legal means. It is not intended as a replacement for existing methods used by lawyers, but rather as a complementary approach. Lawyers already identify and control risks, but our methods and approaches could be

21 See Tobias Mahler, *Legal Risk Management: Developing and Evaluating Elements of a Method for Proactive Legal Analyses, With a Particular Focus on Contracts*, PhD dissertation, University of Oslo, 2010.

better integrated with risk management in other fields, such as, for example, enterprise risk management.

The development of legal risk management raises a number of conceptual challenges. For example, what is «legal risk» and how can it be identified and described? How does legal risk relate to legal uncertainty? These are examples of issues that are addressed in the thesis' conceptual framework.

The thesis presents two elements of a method for legal risk management. First, a legal risk management process is developed based on an existing ISO standard.[22] This process can be used to identify legal and other risks and to assess and treat these in a structured manner.

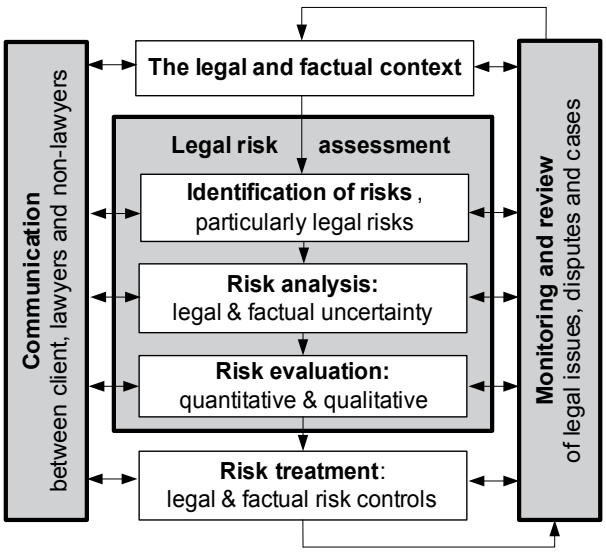


Figure 9: The legal risk management process

The second element is a graphical visualization to support the legal risk assessment. This graphical approach can be employed to draw certain diagrams, which are used to document, assess and treat risks, with a particular focus on legal risks.

The practical utility of the legal risk management method was evaluated through an empirical case study, focusing on a corporation that assessed its

22 ISO, «International Standard Iso 31000. Risk Management--Principles and Guidelines on Implementation,» (2009).

risks related to a major contract. The case study findings suggest that the legal risk management process may indeed facilitate a structured approach to the identification, assessment, and treatment of risk. The graphical language was seen as helpful in communicating risk amongst the case study participants. However, the need for simplicity and usability also leads to some inevitable limitations in analytical capacity. Therefore, the language use may have to be complemented by more detailed legal assessments in natural language.

In its conclusion, the thesis is cautiously optimistic about the future prospects of legal risk management. Legal risk management appears to be feasible, although there are a number of factors that limit the potential use of risk management in the legal context. The thesis results provide a preliminary indication that legal risk management may, under optimal conditions, contribute to improving decision-making about risk in the legal context. As mentioned above, Susskind sees the legal risk manager as one of the five future roles of lawyers. Indeed, I would tend to agree that legal risk management has a considerable future potential, even though a number of challenges are not resolved. Thus, it remains to be seen if we will witness the development of this new role within the next ten years.

Concluding remarks

Regrettably, I can offer no exact prognosis of how lawyers will work in 2020. However, given the speed of developments, the least likely alternative is that tomorrow's lawyers will be just like today's. There are on-going technological innovations, and some of the early applications can already be seen today. Nothing seems to indicate that the technological change will stop in the proximate future. The Web 3.0 is currently being developed, and lawyers will use it to provide their services. In addition, there is an emerging demand for other innovations. In the short run, globalization would seem to imply a considerable increase in complexity in the material with which we lawyers work. Moreover, lawyers could increasingly be asked to adopt new methods and approaches that have proven successful in other disciplines, such as risk management.

If we want to prepare for this future, we can start today. And some have already started. For example, the NRCCL[23] and SITAS[24] have considerable experiences with what above was called legal knowledge engineering. Moreover, the Faculty of Law of the University of Oslo has a clear focus on

23 Norwegian Research Center for Computers and Law.

24 Section for Information Technology and Administrative Systems at the Faculty of Law, University of Oslo.

internationalization in its strategy. And, this faculty even participates in offering an MA degree in risk management and maritime insurance, even though the risk management seems currently to be taught outside the faculty.

Thus, it is tempting to conclude with the science fiction writer William Gibson's words [25] that the future is already here - it is just unevenly distributed.

25 William Gibson in «The Science in Science Fiction», *Talk of the Nation*, NPR, 30 November 1999.

SERI I ET BIBLIOGRAFISK PERSPEKTIV[1]

Anne Gunn Bekken

I forbindelse med at SERI fyller 40 år nå i 2010 er det påbegynt et bibliografiarbeide, dvs. et forsøk på å få en tilnærmet samlet oversikt over det som er skrevet og utgitt av personer tilknyttet SERI gjennom tidene. Det er snakk om store mengder, og det er et tidkrevende arbeide som på dette tidpunkt er i en en startfase. Men ut fra materialet som er samlet inn til nå, skal jeg gi en overfladisk oversikt over SERI i et bibliografisk perspektiv.

Først vil jeg si litt om hvilke skriftserier SERI selv er utgiver av. Deretter gjennomgår jeg de enkelte tiårene og ser på om det er noen emner som dominerer og gir noen eksempler på hva som ble publisert. Jeg har også prøvd å se på om det er noen utvikling i internasjonal publisering gjort av senterets medarbeidere. Til slutt følger en liste over avlagte doktor-, licensiat el. PhD-grader ved SERI.[2]

Serier

I 1971 ble første hefte i **Skriftserien Jus og EDB** utgitt. Fram til 1981 ble det utgitt 48 hefter i serien.

Skriftserien ble i 1981 avløst av **Complex,** hvor det til nå er kommet 270 utgivelser.[3] Her utgis alt fra små studentavhandlinger til doktoravhandlinger , samt rapporter og annet som ikke har andre naturlige publiseringskanaler.

De studentarbeidene som publiseres i Complex lånes mye ut og de blir også ofte utsolgt slik at det må trykkes opp nye. Dette er særlig fordi studentavhandlingene angår tidsaktuelle temaer som ellers ikke har en samlet og tilgjengelig fremstilling.

Ved Avdeling for forvaltningsinformatikks oppstart i 1994 ble det startet en ny serie, **Forvaltningsinformatisk notatserie.** Serien ble strengt tatt etablert før avdelingen idet første hefte ble utgitt allerede i 1993. Det er pr. mars 2010 utgitt 76 titler i denne serien. Den utgis i elektronisk form på nettet, og hefter utgitt fram til 2000 kom også i trykt versjon.

---

1 Innlegg holdt på «**Senter for rettsinformatikk 40 år» seminar 19.mars 2010**»

2 I listen er også PhD-grader avlagt i løpet av 2010 tatt med.

3 Pr. 19.03.10

70-tallet

Hva skrev de om, pionerene, på 70-tallet?

Det er to tema som peker seg ut; personvern og rettsteknologi.[4] I tillegg er det også noen få publikasjoner om Dataprogrammer – rettslige spørsmål, og de berører også så vidt immaterialrettsspørsmål og kontraktsrett.

Som eksempler på utgivelser fra denne perioden passer det å nevne to verk som representerer de to hovedtemaene man forsket på på 70-tallet.

I 1977 kom boken «*Data og personvern*», redigert av Knut Selmer og Ragnar Dag Blekeli. Dette ble raskt en sentral bok, og den er fremdeles i bruk. Juridisk fakultetsbibliotek har 8 eksemplarer av boken, og av disse er 4 utlånt pr. i dag. I biblioteketes arbeidssystemer viser det seg at minst 2 eksemplarer er tapt – dvs. sannsynligvis stjålet av ivrige personvernentusiaster.

Innen rettsteknologitemaet ble Jon Bing og Trygve Harvolds bok «*Legal Decisions and Information Systems*», utgitt på Universitetsforlaget i 1977. Den fikk samme år «Norwegian Royal Academic Gold Medal».

Hoveddelen av publikasjonene på 70-tallet var på norske forlag og i norske tidsskrift. Bing og Harvolds bok viser at det også ble publisert på et annet språk enn norsk. Vi finner også flere artikler i utenlandske tidsskrifter (primært engelskspråklige), og en del konferansebidrag til internasjonale konferanser.

Ingen dr.avhandlinger ble innlevert dette tiåret.

80-tallet

På 80-tallet skrives det fremdeles mye om både personvern og rettsteknologi. Innen rettsteknologi er det mest fokus på informasjonssystemer, og i den forbindelse er det stor produksjon av litteratur angående tekstsøking og mer språkvitenskaplig stoff.

Av nye tema det skrives om kan nevnes datakriminalitet, elektronisk betalingsformidling, det skrives en del mer om opphavsrett enn tidligere, litt om regelforenkling, medierettslige spørsmål, telekommunikasjon, , kunstig intelligens, juridiske ekspertsystemer. De siste punktene hører vel kanskje hjemme under rettsteknologi, men er tatt med her fordi det er temaer som kommer mest på slutten av 80-tallet.

I 1981 ble den første Complexen utgitt, og den var skrevet av Johs. Hansen og hadde tittelen «*Et EDB-system for analyse av rettslige avgjørelser : mate-*

4 Med rettsteknologi menes her bruk av informasjonsteknologi i diverse juridiske sammenhenger. Det kan være enten være juridiske informasjonssystemer hvor man ser på lagring, søking, gjenfinning, eller bruk av saksbehandlingsverktøy eller spesiell programvare i forvaltningen.

matisk grunnlag og utforming av systemet.» Dette var faktisk en hovedoppgave i informatikk, noe som nok viser IRI/SERIs evne til og interesse av å se til andre fagområder og knytte til seg ressurspersoner derfra.

I 1984 kom første bok på et internasjonalt forlag. Det var «*Handbook of legal information retrieval* « hvor Jon Bing var hovedredaktør, i samarbeid med Tove Fjeldvig, Trygve Harvold og Robert Svoboda. Den ble utgitt på forlaget North Holland i Amsterdam.

Det publiserers fremdeles primært på norske forlag og i norske tidskrifter. Av det som publiseres utenlands ser det ut til å være en økning i antall konferansebidrag som publiseres i proceedings. En forklaring på denne spesielle økningen kan være at senteret nå har etablert seg som et betydningsfullt forskningsmiljø i internasjonal sammenheng.

I 1982 publiseres den første dr.avhandlingen, Jon Bings «*Rettslige kommunikasjonsprosesser – bidrag til en generell teori*» som utgis på Universitetsforlaget. Og i 1984 avlegger Mette Borchgrevink sin licsensiatgrad med tittelen «*Ny teknologi i arbeidslivet – rettslige aspekter*». Den utgis på Universitetsforlaget i 1985.

90-tallet

På 90-tallet begynner det å bli vanskeligere å si at det noe tema som dominerer, slik som på 70- og 80-tallet hvor personvern og rettsteknologi ganske tydelig dominerte. Men det er et aktivt forskningsmiljø når det gjelder juridiske ekspertsystemer, kunstig intelligens etc, så det skrives ganske mye på det feltet.

Det man ser er at det skrives mye mer om opphavsrett, telekommunikasjon og medierett enn tidligere. Afin etableres i 1994 og det skrives nok enda mer enn tidligere om offentlig forvaltning og bruk av informasjonsteknologi, samt rettslige konsekvenser av dette. Andre temaer det skrives om er tilgang til offentlig informasjon, og temaer som elektronisk marked, elektronisk handel og EDI kommer for fullt. På midten og slutten av tiåret utgis det også en del om ytringsfrihet.

Som eksempler fra 1990-tallet kan det trekkes frem to studentarbeider som fikk ganske stor oppmerksomhet. Det første er fra 1995 – Knut-Magnar Aanestad og Tormod S. Johansen skrev avhandlingen «*Innsynsrett i elektronisk post i offentlig forvaltning*». Dette var noe av det første som ble skrevet om elektronisk post og internettrelatert stoff. Den ble utgitt i Complex 1/96.

Den andre som fikk kanskje enda mer oppmerksomhet og som har fått nærmest en klassisikerstatus, er «*Opphavsrett i en digital verden*» av Anders Wagle og Magnus Ødegaard. Den ble utgitt på Cappelen Akademisk forl. 1997. Det var en etterlengtet bok, endelig kom det en samlet fremstilling om

dette temaet på norsk. Den har vært pensum frem til for få år siden, og den er fremdeles i bruk i følge utlånsinformasjon fra Bibsys.

Publiseringen i denne perioden viser mye av det samme som tidligere, altså mest norsk, men det kan se ut som det er en økning i publisering i utenlandske tidsskrift og artikkelsamlinger. Det kan sikkert være mange forklaringer på det, og en kan være at temaene blir mer internasjonale.

Antall doktoravhandlinger dette tiåret er økt til 5.[5]

2000-tallet

På 2000-tallet er vi over i informasjonssamfunnet. Heller ikke her kan man si at det er et el. flere tema som dominerer, det er mer en overbygning som dominerer – Internett. Det skrives selvfølgelig om temaer som ikke er knyttet til internett og informasjonssamfunnet, men det er absolutt denne type temaer som dominerer. Eksempler på temaer er opphavsrett (for eksempel fildeling), personvern, redaktøransvar, domenespørsmål, jurisdiksjon, lovvalg, spam, e-forvaltning, internet governance.

Blant publiseringene som ikke tar opp rettslige spørsmål ifht internett ser man at det holdes fremdeles fast i tradisjonen innenfor rettsteknologi. Det kommer arbeider om juridiske informasjonssystemer, det utgis en del i forbindelse med et prosjekt som går på it-støtte for arbeid med lovsaker, og også juridisk risikoanalyse kan man si hører inn under denne tradisjonen.

Når det gjelder personvern som har vært et sentralt tema helt fra starten blir det nå en økning i publiseringer igjen etter en liten nedgang på 1990-tallet

Som et eksempel på det som nevnes tidligere om studentarbeider kan Dana Cojocarasus masteroppgave *«Anti-spam legislation between privacy and commercial interest : an overview of the European Union legislation regarding the e-mail spam»* trekkes frem. Denne oppgaven er populær, lånes mye ut, og den er tydelig interessant utover Norges grenser. Den er blitt trykket opp i nye opplag flere ganger pga. stor etterspørsel.

Det andre eksemplet fra dette tiåret blir boken *«Internet Governance»* redigert av Jon Bing og Lee Bygrave. Den ble utgitt på Oxford University Press januar 2009.

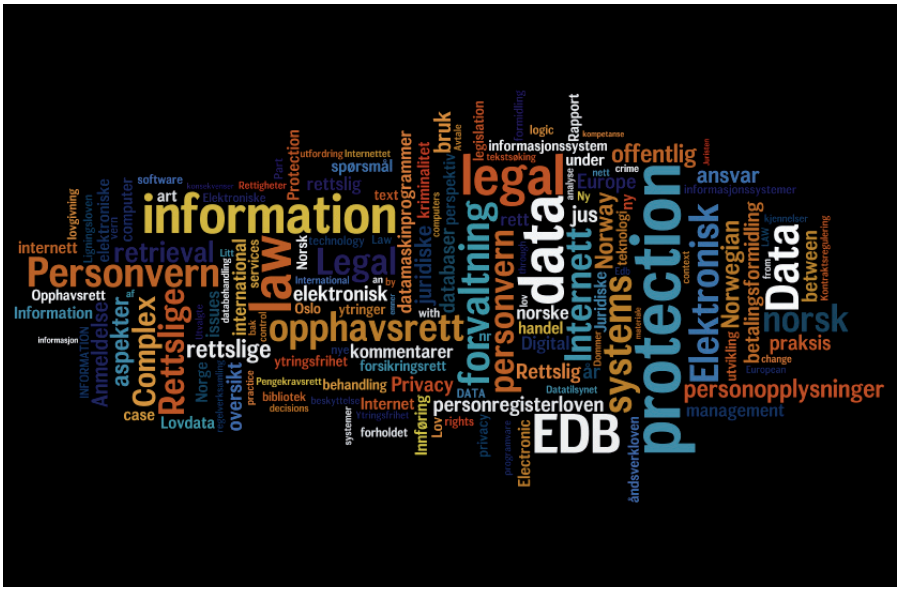
I tråd med eksemplene over, så er det nå stor økning i internasjonal publisering eller publisering på engelsk. Det er mest økning når det gjelder artikler, men også en del bøker utgis på engelsk og på utenlandske forlag.

Det er en betydelig økning i materiale som skrives på engelsk generelt, også flere studentoppgaver skrives på engelsk.

5 Se under for en samlet liste over doktor-, licensiat og PhD-avhandlinger

Dette tiåret avlegges det 8 doktorgrader. Hvis man ser på økningen av avlagte doktorgrader, er det jevn økning fra tiår til tiår. Det starter med 2 stykker på 80-tallet, fortsetter med 5 på 90-tallet og 8 fra 2000-2009. Utfra disse forholdstallene skulle det tilsi at det skal bli 11 i neste tiår (2010-2019). Med de 6 som disputerer i 2010 er man godt på vei til å nå dette antallet.

Oppsummering



Denne noe uredigerte «ordskyen» viser hvilke ord som er mest hyppige i titlene i mitt materiale. Personvern i ulike varianter dominerer, men også «information», «legal» og «systems», altså rettsteknologien, er ganske fremtredende. Dvs. at disse to temaene har vært sentrale helt siden begynnelsen i 1970 og det er ingen grunn til å tro at de ikke vil være det i tiden fremover også.

Doktor-, licensiat- og PhD-avhandlinger 1982-2010

- 1982: Rettslige kommunikasjonsprosesser : bidrag til en generell teori / Jon Bing
- 1984: Ny teknologi i arbeidslivet : rettslige aspekter / Mette Borchgrevink
- 1993: Betalingsformidling i et rettslig perspektiv / Olav Torvund

- 1993: Rettssikkerhet og systemutvikling i offentlig forvaltning / Dag Wiese Schartum
- 1996: Formal theories of rights / Henning Herrestad
- 1997: Normative structures in natural and artificial systems / Christen Krogh
- 1999: Data protection law : approaching its rationale, logic and limits / Lee A. Bygrave
- 2000: Datamaskinprogrammer og skatt : utgiftsføring, aktivering og avskrivning ved inntektsbekatningen / Gjert Melsom
- 2002: Ytringsfrihet : vernet om ytringsfriheten i norsk rett / Kyrre Eggen
- 2006: Schengen Information System and border control co-operation : a transparency and propertionality evaluation / Stephen Kabera Karanja
- 2006: Digitale sertifikater og sertifikattjenester - roller, oppgaver og ansvar : en tillitsorientert tilnærming til sertifikatutstederens villedningsansvar / Rolf Riisnæs
- 2007: Theory and practice of telecommunications regulation in Nigeria through the development question / Peter Chukwuma Obutte
- 2008: Vitenskapsteoretiske og moralfilosofiske grunnproblemer i en postrettsrealistisk norsk rettsvitenskap / Jens Petter Berg
- 2008: Electronic alternative dispute resolution : increasing access to justice via procedural protections / Susan Schiavetta
- 2009: Digital privatkopiering : analyse av åndsverkloven § 12 i møte med tekniske beskyttelsessystemer og rettslige omgåelsesforbud / Thomas Rieber-Mohn
- 2010: Personvernøkende identitetsforvaltning / Thomas Olsen
- 2010: E-commerce contracting : the effective formation of online contracts / Maryke Silalahi Nuth
- 2010: Legal risk management : developing and evaluating elements of a method for proactive legal analyses, with a particular focus on contracts / Tobias Mahler
- 2010: Bio-privacy : legal challenges for privacy regulations of biometric identification and authentication / Yue Liu
- 2010: Tilgang til og videreformidling av helseopplysninger : regulering og kontroll på tvers av IT-systemer og organisatoriske grenser / Herbjørn Andresen
- 2010: Between contract and partnership : dynamic networks as collaborative contracts and more / Emily M. Weitzenboeck
- 2010: Automatisert inndragning / Inger Marie Sunde

PHD AVHANDLINGER / PHD THESES 2010

Thomas Olsen – Personvernøkende identitetsforvaltning (Privacy enhancing identity management)

Sammendrag

Avhandlingens overordnede problemstilling er hvilke krav personopplysningsretten stiller til elektronisk identitetsforvaltning. I all hovedsak omhandler identitetsforvaltning det å identifisere, autentisere og autorisere brukere av tjenester på Internett. Avhandlingen drøfter identitetsforvaltningens grunnleggende utfordringer og begreper, og viser hvordan enkelte av utfordringene kan løses innenfor rammene av såkalt relasjonsorientert identitetsforvaltning. Drøftelsene tar utgangspunkt i en dominerende teknisk standard (SAML), og implementasjonen av denne i sentrale norske e-forvaltningsløsninger som Altinn, Minside/MinID og Feide. Relasjonsorientert identitetsforvaltning innebærer at en identitetsforvalter etter brukerens initiativ og ønske formidler relevante brukeropplysninger til en eller flere tjenesteytere. Fordelene som ofte assosieres med relasjonsorientert identitetsforvaltning er blant annet at brukeren kan få tilgang til flere tjenester gjennom én autentisering hos identitetsforvalter (single sign-on).

Løsninger for relasjonsorientert identitetsforvaltning er grunnleggende for å realisere politiske ambisjoner om økt elektronisk samhandling samt sømløse og integrerte tjenester på tvers av forvaltningens organisering og ansvarsområder. En viktig forutsetning for å kunne nå slike målsetninger er imidlertid at nye løsninger ikke går på bekostning av den enkeltes personvern, og at personopplysningsrettens krav overholdes.

Avhandlingen reiser tre rettslige hovedproblemstillinger angående (i) personopplysningslovens personopplysningsbegrep, (ii) lovens krav til roller og oppgaver og (iii) lovens krav til brukermedvirkning og kontroll. Den første problemstillingen gjelder hvorvidt brukeropplysningene tjenesteyter mottar fra identitetsforvalter skal anses som personopplysninger slik at personopplysningsloven kommer til anvendelse. Til tross for at standarder for relasjonsorientert identitetsforvaltning gjør det mulig å legge til rette for at brukeren kan opptre mer eller mindre anonymt overfor tjenesteyteren, argumenteres det for et vidt personopplysningsbegrep kombinert med mulighet for mer lemplig an-

vendelse av regelverket i tilfeller hvor personvernrisikoen er liten. I forhold til avhandlingens andre hovedproblemstilling drøftes hvilke vurderingsmomenter som er relevante for å vurdere hvorvidt aktørene er behandlingsansvarlige eller databehandlere for de behandlinger identitetsforvaltningen involverer. Den siste problemstillingen gjelder hvilke krav personopplysningsretten stiller til brukermedvirkning og kontroll, herunder hvordan kravene til samtykke og informasjon kan gjennomføres på måter som best ivaretar reglenes formål om selvbestemmelse vedrørende egne personopplysninger.

Avhandlingen bidrar også til den rettspolitiske debatten om personvernøkende teknologi. Det argumenteres i den forbindelse for at en klargjøring av hva tjenesteyteren trenger å få autentisert (f. eks. brukerens identitet, rolle eller egenskap) kan bidra til å fremme brukernes personvern ved at omfanget av utvekslede opplysninger begrenses til det strengt nødvendige.

Summary

The overarching question the thesis raises is what requirements data protection law imposes on electronic identity management. The core elements of identity management include the identification, authentication and authorisation of users of services on the Internet. The thesis analyses the main challenges and terminology related to identity management, and shows how federated identity management can solve some of these challenges. The point of departure for the analysis is a dominating technical standard (SAML) and its implementation in key Norwegian e-Government services such as Altinn, Mypage/MinID and Feide. Federated identity management is characterised by an identity provider's role, which consists of disclosing relevant user information to a service provider in accordance with the users' instructions. One of the advantages often associated with federated identity management is the users' possibility of accessing several service providers' services after a single authentication by the identity provider (single sign-on).

Federated identity management services are significant for realizing political ambitions such as increased electronic communication, including seamless and integrated services across the public administration's organisational boundaries. Vital conditions for achieving such goals, however, are that new services must respect individuals' privacy, and service providers must comply with data protection law.

The thesis raises three main legal issues: (i) the meaning of personal data in the Norwegian data protection act, (ii) the act's requirements regarding roles and responsibilities, and (iii) the act's requirements regarding user participation and control. The first issue concerns the extent to which user information

received by a service provider should be considered personal data, rendering the data protection act applicable. The thesis argues for a broad interpretation of the concept of personal data, even in cases when federated identity management facilitates a more or less anonymous use of a service provider's services. The law's consequently wide scope, however, might be combined with a less strict application of certain rules when the risk to the users' privacy is only marginal. In relation to the second issue, the thesis analyses what criteria are relevant for deciding whether the providers of identity management services are controllers or processors. The last issue deals with the data protection law's requirements regarding user participation and control. It focuses on how compliance with the consent and information provision's requirements can ensure individuals' autonomy regarding personal data.

The thesis also contributes to the policy debate on privacy enhancing technologies (PETs). A clarification of what a service provider needs to authenticate (e.g., a user's identity or role, or a relevant attribute) might, by itself, contribute to enhancing users' privacy by limiting the amount of exchanged personal data to what is strictly necessary.

Maryke Silalahi Nuth - E-commerce Contracting: The Effective Formation of Online Contracts (Elektronisk kontraktsinngåelse)

Summary

Taking the Norwegian experience and regulatory frameworks as starting points for the analysis, and supported by the results of a survey of top websites in Norway and internationally, this thesis offers insights into the complexity and legal uncertainties surrounding the formation procedure of online contracts within and across different technologies and technological platforms. The thesis aims to find answers to the question that, for a long period of time, has been discussed in the area of electronic contracting, but remains unanswered: whether the existing (traditional) legal rules are sufficient to address the legal problems created by electronic contract formation and communication of dispositive electronic messages or whether new rules are needed in this area.

The thesis focuses on two main legal issues: (i) attribution and validity of electronic messages as legally binding statements capable of bringing about contracts and (ii) effective communication of electronic statements being decisive of the moment of contract formation.

The thesis finds that there is no generally applicable and practical method that can be used to establish with certainty qualification of an electronic state-

ment as legally binding statement. It is the interplay between different assessment factors in concrete factual situations that leads to the conclusion of a particular legal qualification. Those relevant assessment factors can be determined with reference to the theoretical and doctrinal framework of characteristics of a legally binding statement, the invalidity rules and the consumer protection rules, as well as the analogical application of established logic and reasoning in offline contracting situations to online contracting.

The design of a contracting system has a more significant and intense role in ensuring effective formation of contracts online than in offline contracting situations. The thesis suggests some features to be included in any design of an electronic contracting system to ensure mutuality of assent is obtained through such a system, and accordingly leads to effective formation of online contracts.

Certain electronic conducts within an electronic contracting system are ways to incorporate terms into a contract. The thesis puts forward the principles of adequate presentation of contract terms that should be respected during the electronic contract formation process so to ensure contract terms have operative legal effects upon acceptance. Application of such principles in addition to due consideration of the essentials of valid legal statements and effective communication of online statements will contribute to the successful application of 'the effective electronic contracting model' proposed in the thesis.

The implicit dimensions of technology and their interplay with contract law rules and doctrines are highlighted in the thesis. The technology can improve contracting processes; however it can also put an end to an established (problematic) contracting practice when applied in an online setting. In dealing with legal problems of electronic contracting or in describing those problems formally, it is important in any case to take sufficient account of the ever-changing nature of technology so that a technology-neutral approach and terminology will be employed.

Sammendrag

Avhandlingen tar utgangspunkt i det norske regelverket og rettspraksis, og på grunnlag av resultater fra en gjennomgang av de mest besøkte norske og utenlandske hjemmesidene, gir avhandlingen oversikt over virkelighetens kompleksitet og innsikt i den rettslige uklarheten om inngåelsen av kontrakter online innen og på tvers av forskjellige teknologier og teknologiske plattformer. Avhandlingens formål er å besvare det lenge ubesvarte spørsmålet innenfor temaet elektroniske kontrakter: hvorvidt de gjeldende (tradisjonelle) rettsregler er tilstrekkelige for å løse de rettslige problemstillingene ved elektronisk

avtaleinngåelse og kommunikasjon av elektroniske meldinger med dispositivt innhold, eller om det er behov for nye regler på dette området.

Avhandlingens fokus settes på to hovedproblemstillinger: (i) hvilke egenskaper og aspekter ved elektroniske meldinger kan gi grunnlag for fastsettelsen av elektronisk utsagns bindende virkning, som igjen er avgjørende for å konstantere avtaleinngåelse? og (ii) hvilke aspekter ved kommunikasjon av elektroniske utsagn er avgjørende for fastsettelsen av avtaleinngåelsestidspunktet?

Avhandlingen viser at det ikke foreligger enkle generelt anvendelige regler og metode som med sikkerhet viser at det foreligger et elektronisk utsagn som kvalifiserer som dispositivt utsagn. Samspillet mellom de forskjellige kriteriene i et konkret tilfelle er ofte avgjørende for om det foreligger et bestemt dispositivt utsagn. Disse kriteriene utledes av teorier om dispositive utsagns kjennetegn, reglene om ugyldighet og forbrukervernsreglene, samt tilsvarende anvendelse av resonnamentene rundt (tradisjonell) offline kontraktsinngåelse til online kontraktsinngåelse.

Selve konstruksjonen av et kontraktsinngåelsessystem vil ha en viktigere og mer intens rolle for å sikre effektiv avtaleinngåelse online enn for offline kontraktssituasjoner. Avhandlingen fremhever enkelte elementer som bør være med ved konstruksjonen av et kontraktsinngåelsessystem for å sikre en gjensidig enighet mellom partene og at en bindende elektronisk avtale etableres gjennom systemet.

Enkelte handlinger i et elektronisk kontraktsinngåelsessystem utgjør (sammen) en fremgangsmåte for å inkorporere vilkår i avtalen. Avhandlingen fremhever prinsippene om adekvat presentasjon av kontraktsvilkår som bør respekteres i et slikt kontraktsinngåelsessystem for å sikre at bestemte kontraktsvilkår gis rettslig virkning via aksept. Anvendelse av disse prinsippene i sammenheng med de fundamentale elementene av rettslig bindende utsagn og effektivt kommunikasjon av online utsagn, vil føre til vellykket implementering av 'effektiv elektronisk kontraktsinngåelsesmodel' som presentert i avhandlingen.

Avhandlingen fremhever de indre dimensjonene av teknologien og samspillet med kontraktsretten. De foreliggende/eksisterende teknologiske muligheter kan forbedre avtalemekanismene online, men dagens teknologi kan til og med sette en stopper for etablert (problematisk) kontraktsprosedyre når slik prosedyre anvendes i en onlinekontekst. Når man skal løse rettslige problemstillinger innenfor elektroniske kontrakter eller beskrive disse problemene, er det under enhver omstendighet viktig å ta tilstrekkelig hensyn til at teknologien er under stadig forandring slik at man benytter en teknologi-nøytral tilnærming og terminologi.

Tobias Mahler - Legal Risk Management: Developing and Evaluating Elements of a Method for Proactive Legal Analyses, With a Particular Focus on Contracts. (Juridisk Risikostyring: En metode for proaktive rettslige analyser, med særlig vekt på kontrakter.)

Summary

Risk management, according to the ISO, refers to a set of coordinated activities to direct and control an organization with regard to risk. This thesis assesses the degree to which risk management methods from other disciplines can be usefully adapted to the legal context. As conceived here, legal risk management is not confined to the management of legal risk, but also includes the management of other risk by legal means.

The proposed aim of legal risk management is the adequate management of risk in the legal context. It is not intended as a replacement for existing methods used by lawyers, but rather as a complementary approach. Lawyers already identify and control risks, but our methods and approaches could be better integrated with risk management in other fields, such as, for example, enterprise risk management.

The development of legal risk management raises a number of conceptual challenges. For example, what is legal risk and how can it be identified and described? How does legal risk relate to legal uncertainty? These are examples of issues that are addressed in the thesis' conceptual framework.

The thesis presents two elements of a method for legal risk management. First, a legal risk management process is developed based on an existing ISO standard. This process can be used to identify legal and other risks and to assess and treat these in a structured manner.

The second element is a graphical visualization to support the legal risk assessment. This graphical approach can be employed to draw certain diagrams, which are used to document, assess and treat risks, with a particular focus on legal risks.

The practical utility of the legal risk management method was evaluated through an empirical case study, focusing on a corporation that assessed its risks related to a major contract. The case study findings suggest that the legal risk management process may indeed facilitate a structured approach to the identification, assessment, and treatment of risk. The graphical language was seen as helpful in communicating risk amongst the case study participants. However, the need for simplicity and usability also leads to some inevitable

limitations in analytical capacity. Therefore, the language use may have to be complemented by more detailed legal assessments in natural language.
In its conclusion, the thesis is cautiously optimistic about the future prospects of legal risk management. Legal risk management appears to be feasible, although there are a number of factors that limit the potential use of risk management in the legal context. The thesis results provide a preliminary indication that legal risk management may, under optimal conditions, contribute to improving decision-making about risk in the legal context.

Sammendrag

Risikostyring blir av ISO definert som et sett av koordinerte aktiviteter som bidrar til å styre og kontrollere en organisasjons håndtering av risiko. Avhandlingen tar sikte på å vurdere hvorvidt risikostyringsmetoder fra andre fagområder kan tilpasses slik at de blir nyttige i en juridisk kontekst. Juridisk risikostyring er ikke begrenset til styring av rettslige risiko, men inkluderer også styring av annen risiko ved hjelp av rettslige tiltak.

Målet for juridisk risikostyring bør være å oppnå en hensiktsmessig styring av risiko i en rettslig sammenheng. Metoden er tenkt som et supplement til andre metoder som brukes av jurister, det er ikke meningen å erstatte disse. Jurister arbeider allerede i dag med å identifisere og kontrollere risiko, men metodene og tilnærmingene kunne med fordel integreres bedre med risikostyring på andre områder.

Det å utvikle metoder for juridisk risikostyring innebærer en rekke konseptuelle utfordringer. For eksempel, hva menes med begrepet «rettslig risiko» og hvordan kan slik risiko best bli identifisert og beskrevet? Hva er relasjonen mellom rettslig risiko og rettslig usikkerhet? Disse og andre spørsmål behandles i avhandlingens konseptuelle rammeverk.

Avhandlingen presenterer to elementer av en metode for juridisk risikostyring. Det første elementet er en prosess for juridisk risikostyring, basert på en eksisterende ISO standard. Denne prosessen kan brukes for å identifisere, vurdere og behandle risiko på en strukturert måte.

Det andre elementet er et grafisk språk, som kan brukes for å støtte en rettslig risikovurdering. Ved hjelp av dette språket kan man tegne en bestemt type diagrammer, som kan brukes for å dokumentere identifisert risiko, særlig juridisk risiko. Diagrammene kan også brukes til å estimere en risikoverdi, og til å vurdere alternativer for å behandle risiko.

Avhandlingen beskriver også en empirisk case-studie, der risikostyringsmetoden ble brukt og evaluert i praksis. Resultatene indikerer at prosessen for rettslig risikostyring kan bidra til en strukturert identifisering, analyse og be-

handling av risiko. Det grafiske språket, som ble brukt for å modellere risiko i case-studien, ble av deltakerne evaluert som et nyttig redskap for å beskrive og analysere rettslig risiko. Samtidig var det tydelig at behovet for et brukervennlig grafisk språk innebar forenklinger som begrenser språkets funksjon som analyseredskap. Det kan derfor være nødvendig å supplere diagrammene med rettslige vurderinger i naturlig språk.

Avhandlingens konklusjon er forsiktig optimistisk med hensyn til fremtidsutsiktene for juridisk risikostyring. Tilnærmingen fremstår som gjennomførbar, skjønt det finnes en del faktorer som begrenser hensiktsmessigheten av risikostyring i en rettslig sammenheng. Avhandlingen gir en foreløpig indikasjon på at juridisk risikostyring under optimale forhold kan bidra til å forbedre beslutninger om risiko i juridisk arbeid.

Yue Liu - Bio-privacy: Legal Challenges for Privacy Regulations of Biometric Identification and Authentication

Summary

The main objective of the thesis is to find out what are the privacy issues raised by the use of biometric technology and what might be the appropriate legal solutions? Characteristics of biometric information and examining legal safeguards which exist on national and EU levels has been analyzed, with the aim of recommending appropriate safeguards in order to provide adequate human rights and personal data protection. The fundamental idea on which the thesis is based is that an interaction exists between biometric technology and privacy protection. The consequences of biometric technology development will unavoidably affect the function and nature of privacy protection. The legal measures of privacy protection could, however, be adjusted according to the challenges posed by the technology, and so ensure that the technology be used in a privacy-friendly manner. To achieve the central objectives of this thesis, four sets of sub-questions were investigated: 1) what are the privacy issues in the biometric context? 2) How are these issues dealt with under the law currently? What principles are applied? What interests are served? 3) Is current regulation satisfactory? Does it facilitate a fair weighting of the diverse interests involved? Is it sufficiently clear? Is it applied consistently? 4) Generally, what is the most appropriate approach to deal with the legal challenges posed by the use of biometrics? These sub-questions are dealt with in different parts of the thesis, and the answers to each provide the results that I delineate in the conclusion.

Herbjørn Andresen – Tilgang til og videreformidling av helseopplysninger : regulering og kontroll på tvers av IT-systemer og organisatoriske grenser (Access to and desclosure of medical data)

Sammendrag

Avhandlingen er en tverrfaglig analyse av mulighetene for å kontrollere tilgang til helseopplysninger, med særlig vekt på de sammenhengene der ulike aktører har behov for de samme opplysningene. Hovedperspektivet er berettiget tilgang og videreformidling, altså den bruk av opplysninger som normalt skal eller bør finne sted. Det innebærer også at analysens mål først og fremst er å vurdere mulighetene for hensiktsmessig kontroll av de store datavolumene. Atypiske tilfeller og særskilt kompliserte gråsoner vies mindre oppmerksomhet.

Det sentrale forskningsspørsmålet er «hvilke teknologiske representasjoner er best egnet til å uttrykke og håndheve ulike sider ved reguleringen av tilgang til og videreformidling av helseopplysninger»? Denne reguleringen har to hovedkomponenter. Den ene er generelle krav til tilgangskontroll som en del av virksomhetens informasjonssikkerhetsarbeid, den andre er konkrete regler om når det kan gjøres unntak fra taushetsplikten, og på hvilke betingelser.

Kravene til informasjonssikkerhet er forankret i personopplysningsretten, og basert på internkontroll som reguleringsmetode. Denne formen for regulering gir prosessregler som er svært fleksible, og gir virksomhetene stort handlingsrom. Taushetsplikten, som primært er regulert i helsepersonelloven, er i utgangspunktet individuell. Den binder hver enkelt som behandler helseopplysninger. Unntakene er i prinsippet uttømmende regulert, selv om det i praksis ligger noe fleksibilitet i at det ofte er en skjønnsmessig vurdering hvorvidt en unntakssituasjon faktisk har inntruffet.

I avhandlingen legges det vekt på å tydeliggjøre forskjellene mellom disse to hovedkomponentene i reguleringen, selv om det også trekkes frem enkelte forhold som minsker avstanden mellom dem. Et forhold som minsker denne avstanden er at virksomhetene er pålagt å sørge for å legge til rette for at taushetsplikten blir overholdt. Et annet slikt forhold er at det både innen personopplysingsretten og helseretten finnes begrensede, men viktige, rettigheter til kontroll og medvirkning for pasienten. Likevel er det avstanden mellom disse to hovedkomponentene som er mest slående.

Den teknologiske innfallsvinkelen i avhandlingen er en drøfting av autorisasjonsprinsipper, og hvordan de ulike trekkene ved reguleringen kan representeres i tilgangskontrollmekanismer. Beskrivelsene av representasjonsmåter

er lagt på et relativt generelt nivå, og ikke knyttet til konkrete produkter eller implementasjoner. Autorisasjonsprinsippene er vurdert og sammenlignet ut fra kriterier som er utarbeidet og begrunnet gjennom avhandlingens innledende deler. Hvert av prinsippene har sterke og svake sider, ingen av dem peker seg ut som overlegent bedre enn de andre.

Summary

The thesis is a cross-disciplinary analysis of the possibilities for controlling access to personal health data, in particular when different institutions or health care professionals need access to the same set of data. The thesis concentrates on legitimate data access and disclosure, thus implicating that the analysis primarily assesses the possibilities for suitable and sufficient ways to control the flow of health data at large. Unusual cases or particularly complicated grey areas are paid minor attention.

The primary research question is «what kind of technological representations will express and enforce the regulations pertaining to health data access control in the most optimal way»? These regulations can be divided into two main components. One is the enterprise's access control requirements, which are part of the information security regulations. The other is the relevant legislation regulating exceptions to the general secrecy obligations of the medical professions.

The information security regulations are laid down in data protection law, and they are based on internal control as a methodological principle. Thus information security regulations are flexible procedural rules that allow individual enterprises to work out their own risk assessments and control measures to a certain degree. On the other hand, the secrecy obligation, as laid down in the Health Personnel Act, is an individual obligation on each person who process personal health data. The exceptions to the secrecy obligations are exhaustive, although some flexibility can be read into the fact that there is often a discretionary assessment whether a situation calling for an exception to the secrecy obligation has actually occurred.

The thesis puts a large emphasis on elucidating the differences between these two main components of the relevant regulation. Yet, some circumstances are also described which diminish the differences between them. One is the enterprise's obligation to see to it that the conditions are favourable for compliance with the individuals' obligations of secrecy. Another circumstance is that both data protection law and health law provides limited, yet important, means for the patients themselves to decide or participate in decisions concer-

ning processing of their personal data. Still, the differences between these two components of regulations are more striking than their similarities.

The technological approach of the thesis is a comparison of authorization principles, discussing how the regulations can be represented in access control mechanisms. The different ways of representing authorizations are described at a general level. The different authorization principles are assessed and compared on the basis of criteria which are compiled and motivated throughout the opening parts of the thesis. Each principle has both strengths and weaknesses. Different principles are more or less suited for different purposes or concerns, but no single principle appears to be outstanding or superior.

Emily Weitzenboeck - Between contract and partnership: Dynamic networks as collaborative contracts and more (Mellom kontrakt og selskap: Dynamiske nettverk som samarbeidsavtaler og mer)

Summary

The growth of information and communications technology has fostered the development of new forms of entrepreneurial co-operation such as dynamic networks. The last two decades have witnessed a trend towards the disintegration of large firms and their reorganisation into smaller units, focusing on core competencies and outsourcing the other areas of business. In dynamic networks, small and medium businesses, including freelancers, link up together or with larger firms and form networks that respond quickly to business opportunities. These networks are often hybrid, having elements of both contract-based organizations and corporate forms, in particular partnership. The thesis examines the relative utility of contract and partnership law in fostering and maintaining these emerging business models.

The thesis proposes a threefold categorisation of dynamic networks: (i) spontaneous and temporary virtual enterprises, (ii) virtual enterprises that are created for a limited time out of a pre-established pool of firms, and (iii) long-term dynamic networks with a lead partner. These different types of dynamic networks are used to examine whether and how contract and partnership law regulate and cope with such networks.

This thesis directs its focus on that area where contract and partnership law intersect, that is where these disciplines overlap. It seeks to examine the reason for this overlap which, very often, is because one discipline supplements or «fills in gaps» left blank by the other.

Basic questions of contract law are examined, such as the notion of contract and why parties use contract as a regulatory tool. The classical theory's view of contract as a discrete transaction characterised by simultaneous exchange between antagonistic parties is problematic for dynamic networks where the parties need to collaborate to achieve the scope for which that network was set up for. The thesis has therefore looked at modern contract law theory for a different perspective of contract. Since dynamic networks may not only be created through the use of one multilateral contract but also through a series of contracts, the notion of contractual networks is also examined.

Though most dynamic networks are set up on the basis of a contract or a series of contracts, certain overriding rules in national partnership law may nevertheless still apply. An analysis is made of the consequences that could ensue where a relationship that parties had intended to set up as «merely» contractual is deemed to be a partnership in terms of mandatory law, viz: (i) personal liability towards third parties, (ii) fiduciary duties and (iii) limitations on the expulsion, withdrawal and admission of members, as well as dissolution of the partnership.

A closely related question, which plays a central role in this thesis, is the behaviour of the parties in such networks. The notion of good faith and its various nuances, as a behavioural criterion in contractual and partnership relations, is an important and recurring theme which is discussed and probed in a large part of this thesis.

To analyse the legal framework used by businesses to set up dynamic networks in practice, an empirical study was carried out and a number of real examples of dynamic networks from different countries were examined. The thesis takes account of legal rules in a number of jurisdictions, in particular, England, Norway, Italy, France and Germany.

Sammendrag

Utviklingen innenfor informasjons- og kommunikasjonsteknologi har resultert i en oppblomstring av nye typer modeller for samarbeid mellom bedrifter. Dynamiske nettverk er et eksempel på dette. De to siste tiårene har vi sett en trend mot oppløsning og omorganisering til mindre enheter i de store bedriftene. Det blir fokusert på kjernekompetanse, og de andre delene av virksomheten blir gjerne outsourcet. Dynamiske nettverk muliggjør at små og mellomstore bedrifter, samt frilansere, kan samarbeide på tvers, for deretter å bruke kompetanseutvidelsen dette medfører til lettere å oppdage og videreutvikle nye forretningsmuligheter. Disse nettverkene er ofte «hybrider» som inneholder elementer av både kontraktsbaserte samarbeidsenheter og selskaper, og

da spesielt ansvarlige selskaper. Avhandlingen tar for seg den relative nytten kontraktsrett og selskapsrett kan gi til å fremme og opprettholde disse nye forretningsmodellene.

Avhandlingen foreslår en tredelt inndeling av dynamiske nettverk: (i) spontane og midlertidige virtuelle bedrifter, (ii) virtuelle bedrifter som er opprettet for en tidsbegrenset periode på bakgrunn av en forhåndsdefinert «pool» av bedrifter, og (iii) langsiktige dynamiske nettverk med én hovedpartner. Disse ulike typene av dynamiske nettverk brukes til å undersøke om og hvordan kontraktsrett og selskapsrett behandler og regulerer slike nettverk. Videre fokuseres det på skjæringspunktet mellom kontraktsrett og selskapsrett, altså der disse rettsområdene overlapper og krysser hverandre. Avhandlingen ser på årsaken til denne overlappingen, som ofte skyldes at det ene rettsområdet supplerer eller utfyller det andre.

Det blir også sett nærmere på grunnleggende kontraktsrettslige spørsmål, for eksempel hva en kontrakt er, og hvorfor partene velger nettopp kontrakt som regulatorisk verktøy. Den tradisjonelle kontraktsretten er i de fleste tilfeller basert på en kontrakt mellom parter med kryssende interesser, der man typisk har en samtidig utveksling og oppfyllelse av plikter etter avtalen. Dette vil fungere dårlig i et dynamisk nettverk, idet partene er avhengig av å samarbeide for å oppnå nettverkets formål. Avhandlingen ser derfor på den mer moderne kontraktsretten, for å få et bredere perspektiv på hva en kontrakt er. Siden dynamiske nettverk kan oppstå ikke bare som følge av en flersidig avtale, men tidvis også på grunnlag av flere kontrakter, er slike kontraktsbaserte nettverk også undersøkt.

Selv om de fleste dynamiske nettverk er basert på en eller flere kontrakter, vil visse ufravikelige regler i nasjonal selskapsrett likevel kunne komme til anvendelse. Avhandlingen analyserer virkningene av overgangen mellom et forhold som partene hadde ment skulle være kun kontraktsmessig, og når dette juridisk sett kan ansees som et selskap, nemlig (i) personlig ansvar overfor tredjemann, (ii) økt lojalitet mellom kontraktspartene, og (iii) begrensninger på muligheten for å ekskludere partnere, trekke seg ut av samarbeidet, ta inn nye partnere og for å oppløse samarbeidet.

Et nært beslektet spørsmål som spiller en sentral rolle i avhandlingen, er partenes adferd i slike nettverk. Læren om ulike grader av lojalitet som kriterium i kontrakts- og selskapsforhold, er et viktig og stadig tilbakevendende tema som blir diskutert og grundig analysert i avhandlingen.

Det ble videre utført en empirisk studie der flere reelle eksempler på dynamiske nettverk fra ulike land blir systematisk gjennomgått, med det formål å analysere de juridiske verktøyene som bedriftene bruker i praksis for å danne

nettverkene. Avhandlingen tar for seg regelverket i en rekke jurisdiksjoner, men med særlig vekt på reglene i England, Norge, Italia, Frankrike og Tyskland.

Inger Marie Sunde – Automatisert inndragning (Confiscation by Automation)

Sammendrag

Kan politiet sette opp et filter på internett og inndra alle barnepornobilder som fanges opp av filteret? Dette er et av spørsmålene som behandles i Inger Marie Sundes doktoravhandling.

Avhandlingen analyserer gjeldende rett for inndragning av datafiler. Hovedspørsmålet er om reglene åpner for filtrering av ulovlig innhold på internett. Dette er praktisk for eksempel for datafiler med overgrepsbilder av barn (også kalt «barnepornografi») og datafiler med skadelig dataprogram som «datavirus», «orm» og «trojaner».

Inndragning er en strafferettslig reaksjon som både kan idømmes alene og ved siden av straff som fengsel og bot. Straffeloven gir adgang til å inndra «ting». Inndragning innebærer at tingen fratas lovbryteren med varig virkning. Inndragning kan rettes både mot fysiske og immaterielle objekter som narkotika, pengesedler, datautstyr, rett til fast eiendom og pengekrav.

Avhandlingen konsentrerer seg om to hovedtema. Først drøftes om datafiler som er tatt i beslag av politiet kan inndras. I praksis er det tale om datafiler som er lagret på beslaglagt datautstyr m.v.. Spørsmålet er altså om politiet kan inndra barnepornobilder m.v., som de finner på en PC som er beslaglagt hos en mistenkt. Behandlingen involverer en bredere drøftelse av de strafferettslige begrepene «ting» og «gjenstand» i forhold til informasjonsteknologi. Videre vurderes betydningen av teknologinøytralitet som reelt hensyn ved fortolkning av straffeloven. Konklusjonen er at inndragningsreglene gir adgang til å inndra datafilene. Inndragningsbeslutningen kan spesifisere de filer som omfattes ved henvisning til filenes unike tekniske identitet (sjekksummen).

Det andre hovedtemaet er om inndragningsbeslutningen kan anses å omfatte identiske datafiler som er andre steder enn i beslaget, typisk på internett. Dersom et barnepornografisk bilde er besluttet inndratt, kan man da også inndra kopier av dette bildet som er spredt på internett? Det oppstår spørsmål om å gi inndragningsbeslutningen virkning for ukjent eier eller besitter. Identiske datafiler er «dubletter» og har identisk sjekksum. Identiteten fastslås av datasystemene og kan brukes som grunnlag for filtrering. Videre oppstår det spørsmål om det rettslige grunnlaget for at dublettene skulle anses å være inndratt.

Her har avhandlingen to innfallsvinkler: Den ene baserer seg på en parallell til inndragning av bøker, og betydningen av den teknologinøytrale utformingen av inndragningsreglene i straffeloven av 2005. Den andre tar utgangspunkt i at elektroniske data grunnleggende sett har andre egenskaper enn fysiske objekter. Spørsmålet er om det rettslige begrepet «ting» omfatter alle dublettene fordi tid og sted ikke har samme mening på nettet som i den fysiske verden. I så fall kan inndragning av dubletter ved filtrering skje når inndragningsbeslutning er avsagt for en av dem. Avhandlingen konkluderer med at den sistnevnte tilnærmingen har best rettskildemessig forankring, særlig på grunn av sammenhengen med den rettstilstand som er kartlagt under første hovedtema.

Til sist vurderes inndragning i nettet ved filtrering av datafiler i forhold til personvern og ytringsfrihet, jf. EMK art. 8 og 10. Konklusjonen er at disse rettighetene ikke er til hinder for inndragning i nettet. Analysen indikerer også at det foreligger en positiv forpliktelse til å inndra overgrepsbilder i nettet.

Summary

Does the law authorize the law enforcement use a filter on the Internet in order to confiscate electronic files that carry child pornography? This is one of the questions dealt with by Inger Marie Sunde in her phd thesis.

The Norwegian confiscation rules are part of the sanction system in criminal law. The first and fundamental question is whether a computer file may be regarded as an «object» (Norw.: «ting») in the sense of the confiscation rules. If so, next question is whether the confiscation rules form basis for Internet filtering. The question is of practical importance for instance to computer files with images of sexual abuse of children (also called «child pornography»), and to «malware» detrimental to computer and network security.

According to Norwegian criminal law, both physical and intangible goods are «objects» that may be confiscated. Narcotics, cash, computer equipment, title to real estate and economic claims are examples of such objects. Whether the legal term «object» in the confiscation rules may be interpreted so as to encompass a computer file, requires a more general analysis of criminal law, which also uses the expression «item» (Norw.: «gjenstand») which seems to be interchangeable with «object». The analysis includes a discussion of technology neutrality as a principle for interpretation of criminal law provisions.

The conclusion is that computer files may be confiscated according to current legal rules. The files may be specified in the confiscation decision by reference to their unique technical identity, i.e., the check sum (hash value).

The next main question is whether the confiscation decision has legal effect beyond the files in the present case. More precisely, the question is whether

«duplicate files» (i.e. files with the same check sum as the confiscated file) that have been distributed on the Internet may be regarded as confiscated as well. Accordingly, the question arises whether a confiscation decision may be binding to an unknown party who owns or possesses duplicate files. Furthermore, it is a question why the duplicates should be encompassed at all. One possible view is to reason along the lines of confiscation of books and the impact of the technology neutral wording of the confiscation rules in the Norwegian Criminal Code of 2005. Another possible view is that «object» must be given a different meaning in electronic than in physical space, because time and space does not have the same significance on the Net as in the physical world. Thus, «object» may include both the original file and the duplicates, because the technology can treat them as one. The conclusion is that the second option seems to be sound, as it follows the logic of the law analyzed under question number one.

Finally, the thesis considers Internet confiscation in relation to articles 8 and 10 of the ECHR (i.e. privacy and freedom of speech). The conclusion is that confiscation is not in contravention of the fundamental rights. There are also indications of a positive obligation to carry out Internet confiscation of images of sexual abuse of children.

ANSATTE/EMPLOYEES 2010

Andresen, Herbjørn – stipendiat (Research Fellow)
Bekken, Anne Gunn B. – hovedbibliotekar (Head Librarian)
Berg-Jacobsen, Ivar – vit.ass. (Research Assistant)
Bing, Jon – Professor
Bogya, Emese – vit.ass. (Research Assistant)
Bygrave, Lee A. – førsteamanuensis (Associate professor)
Dobos, Eva – avdelingsleder (Head of research administration)
Engen, Ståle – forsker (Researcher)
Eriksen, Siri – førstekonsulent (Senior executive officer)
Fimreite, Laila E. – resepsjonist (secretary)
Grjotheim, Frank – vit.ass. (Research Assistant)
Halvorsen, Gro – førstekonsulent (Senior executive officer)
Jansen, Arild – førsteamanuensis (Associate professor)
Jonassen, Siril – resepsjonist (secretary)
Liu, Yue – stipendiat (Research Fellow)
Mahaidran, Mahadevan – overingeniør (Head Engineer)
Mahler, Tobias – stipendiat (Research Fellow)
Malt, Gert Fredrik – amanuensis (Assistant professor)
Mironenko, Olga – stipendiat (Research Fellow)
Modvar, Eva – kontorsjef (Office manager)
Nuth, Maryke Silalahi – stipendiat (Research Fellow)
Ranheim, Malin – forsker (Researcher)
Read, Darren – vit.ass. (Research Assistant)
Rigvår, Thomas – vit.ass (til 1.juni) (Research Assistant)
Schartum, Dag Wiese – Professor, Senterleder (Director of the Center)
Skjerve, Jon Fredrik – vit.ass. (til 1.juni) (Research Assistant)
Sønneland, Helge – spesialråd (Assistant Secretary General)
Torvund, Olav – Professor
Tranvik, Tommy – forsker (Researcher)
Weitzenboeck, Emily M. – stipendiat (Research Fellow)