Nordisk Tidsskrift for Kriminalvidenskab 2000

GLOBALISERINGEN AV KONTROLL: FREMVEKSTEN AV REGISTRERINGS- OG OVERVÅKINGSSYSTEMER I EUROPA.

AV PROFESSOR DR. PHILOS THOMAS MATHIESEN

*The paper deals with the development of registration and surveillance systems within the context of the policing of the new Europe. A plethora of systems using modern data technology are either on wheels, in the making or being planned. One of them is the Schengen Information System, which is already on line with millions of records about hundreds of thousands of people, together with a vast auxiliary bi-national and multi-national exchange of information through the SIRENE system. Another is the Europol Computer Systems, TECS, which are expected to be on line in 2001, and which will consist of an information system, a number of analysis registers as well as an index system, and which will register a wide range of very sensitive, private and personal data in the analysis registers. A third is the EURODAC finger print system, designed to register finger prints and other information about virtually all asylum seekers in Europe. A fourth consists of plans for surveillance of telecommunications, disclosed in the so-called ENFOPOL papers. The various systems are being integrated, and though there are rules regulating data protection, various factors – including differences between police cultures throughout Europe and the rapid development of data technology – make data protection highly vulnerable. Several of the systems (the Schengen Information System and EURODAC) are in pratice designed primarily to control aliens, not crime. Others (Europol) are designed to combat crime, but are probably not particularly efficient as preventive tools. However, they constitute a great threat to the rights of the individual, and slight change in the political wind may lead to gross misuse. A "control society" of a new kind may seen in the horizon. The development is a part of the general globalization which the world currently undergoes.**

Kjære tilhørere:
Det sies rett som det er at vi har gått over i et "informasjonssamfunn". Jeg er nok litt usikker på den betegnelsen. Vi ser jo ser at "industrisamfunnet" blom-

* Title in English: *The Globalization of Control: The Development of Registration and Surveillance Systems in Europe.* Original in Norwegian, but the author has written an extensive paper on the topic in English: *On Globalisation of Control: Towards an Integrated Surveillance System in Europe,* A Statewatch Publication 1999, available from Statewatch, PO Box 1516, London N16 0EW, UK.

strer som aldri før, med allehånde varer som kjøpes og selges, slik at informasjonsteknologien mer er en ny produktivkraft som befordrer den industrielle samfunnsform. Utover det kunne jeg tenke meg å kalle den medieverden vi lever i – fra tabloidavisene gjennom TV til Internett – vel så mye for et "desinformasjonssamfunn" som et "informasjonssamfunn" (se nærmere Mathiesen 1999). Ikke helt og holdent, for, som jeg kommer til å antyde, har bl.a. forskere nytte av Internett når de skal finne ut av et tema som registrerings- og overvåkingssystemer i Europa. Men i ganske stor grad.

Dessuten gir bildet av "informasjonssamfunnet" oss det inntrykk at informasjonen vi i dag har tilgang på gjør oss både friere og lykkeligere. Vi "surfer" jo på Internett – som om vi var på et uendelig, fritt og blått hav. Vi "surfer" nok, men spørsmålet er om vi blir så frie og lykkelige.

Det bringer meg til temaet for dagens foredrag: Globaliseringen av kontroll – Fremveksten av registrerings- og overvåkingssystemer i Europa. Den fremadstormende informasjonsteknologien blir i stigende grad brukt til å registrere, ja, å overvåke og fotfølge oss. Det gjelder på hele den store private sektor. Det gjelder i den offentlige sektor generelt. Og det gjelder politiet. I det godes navn – og det er klart at informasjonsteknologien og registrene har gode sider – skjer det en farlig, skjult utvikling. At noe har dobbeltkarakter – Karl Marx' gamle begrep – har aldri vært sannere enn i dag.

Det er politiets internasjonale registrerings-og overvåkingssystemer jeg skal si litt om i dag. I løpet av noen år har det vokst fram, eller blitt planlagt, en rekke formidable, grenseoverskridende registrerings- og overvåkingssystemer til bruk i politisamarbeid, som reiser fundamentale rettssikkerhets- og personvernsproblemer.

Først litt om rammen for utviklingen. For 25 år siden advarte Den britiske foreningen for sosialt ansvar i vitenskap (British Society for Social Responsibility in Science, BSSRS) mot en ny undertrykkelsesteknologi som var i ferd med å komme i samband med konflikten i Nord-Irland. I 1977 brakte medlemmer av denne foreningen temaet videre i en bok med tittelen *The Technology of Political Control* (Ackroyd m.fl. 1977). Man analyserte teknologiens rolle og funksjoner som resultat av forskning og utvikling i konflikten i Nord-Irland, Storbritannias siste kolonikrig. Kritikere i såkalte "non-governmental organizations" i USA påpekte samtidig hvordan denne teknologien ble utviklet videre innenfor USAs "militær-industrielle kompleks", ikke minst under Vietnamkrigen.

Den britiske foreningen var den første gruppen av vitenskapsfolk og teknologisk personell som rett ut sa at vi her sto overfor en type teknologi hvis hovedformål var å oppnå sosial og politisk kontroll. I Ackroyd og medarbeideres bok ble uttrykket "den politiske kontrollens teknologi" lansert, og definert som "en ny våpentype". "Den er produktet av anvendelsen av vitenskap og teknologi med sikte på spørsmålet om å nøytralisere statens indre fiender. Den er hovedsakelig rettet mot den sivile befolkning, og er ikke innrettet mot å drepe (og den

dreper sjelden). Den har like mye hjerter og hjerner som kropper som siktemål". Og videre:

> Denne nye våpentypen går fra metoder for å overvåke indre uenighet til teknikker for å kontrollere demonstrasjoner; fra nye avhørsteknikker til metoder for å kontrollere fanger. De tilsiktede og faktiske virkningene av disse nye teknologiske hjelpemidlene er både bredere og mer sammensatte enn de mer dødelige våpnene som de føyer seg til.

Etter hvert har det som Ackroyd og medarbeidere samt andre foregrep og forutsa på 1970-tallet, funnet sted. En rapport fra januar 1998 av Steve Wright, betegnet som et arbeidsdokument og sendt til Europaparlamentets Komité for sivile rettigheter og indre spørsmål sier det slik i korttekst (Wright 1998, s. 2):

> Det har vært noen ganske fryktinngydende endringer i de teknologiene som er tilgjengelige for statsmakten når det gjelder indre kontroll siden den første BSSRS-publikasjonen for et kvart århundre siden. Så mange nye teknologier er blitt skapt at spesialist-publikasjoner har utviklet seg for å betjene det blomstrende markedet.

Mer konkret, sier Wright (s. 6), har det siden 1970-tallet kommet en lang rekke teknologiske nydannelser for politiet, for paramilitære enheter, for etterretningstjenester og for indre sikkerhetsstyrker. Mange av dem har vært resultat av videreutvikling av teknologier som var tilgjengelige på 1970-tallet, mens mange andre – som helt nye midler til telefonavlytting, stemmegjenkjennelse og elektronisk sporing – ikke kunne forutses på 1970-tallet fordi man ikke hadde anelse om at "datakraften som var nødvendig for et nasjonalt overvåkingssystem var oppnåelig."

Generelt har utviklingen, som altså for en stor del startet i det militære, gått i retning av å "øke makten og effektiviteten i politiarbeidet, ..." (s. 6). Selskaper produserer nå våpen og kommunikasjonssystemer for både det militære og politiet, og teknologien benyttet av det militære og av politiet smelter sammen. I økende grad blir slike systemer "muskelen og nervesystemet i enheter ansvarlig for offentlig orden" (s. 8). Wright sier det også slik, i en uttalelse som er av stor interesse for politiforskningen generelt (s. 6, min utheving):

> Et massivt *politi-industrielt kompleks* er blitt født for å betjene behovene til politiet, paramilitære styrker og sikkerhetsstyrker. Det ser vi gjennom antallet selskaper som nå er aktive i markedet.

Omega Foundation, som Wright arbeider for (en menneskerettighetsorganisasjon med sete i Manchester) har detaljer om *over 5.000 forretningsselskaper som er aktive innen det politi-industrielle kompleks* (s. 60).

Det er særlig *overvåkingsteknologien*, som angår oss her i ettermiddag.

Overvåkingsteknologien viser i klartekst hvordan store og tunge institusjoner i samfunnet – både politiske og utøvende myndigheter, og ikke minst politiet –

kan nyttiggjøre seg informasjonsteknologiske muligheter, og bruke disse muligheter som kontrollinstrumenter nedover i samfunnssystemet.

Overvåkingsteknologi defineres av Wright som (s. 16) "utstyr eller systemer som kan ha oppsyn med [monitor], forfølge og vurdere bevegelsene til individer, deres eiendeler eller andre verdier". Det gjelder databaserte registrerings- og overvåkingssystemer, såkalte CCTV-overvåkingsnettverk (closed circuit television, internfjernsyn), teknologi for gjenkjennelse av ansikter, systemer for gjenkjennelse av motorkjøretøy, rom- og kommunikasjonsavlyttingsutstyr, nasjonale og internasjonale avlyttingsnettverk. Opp til 1960-tallet var det meste av den overvåking som fant sted i politimyndigheters regi lavteknologisk og dyr. Selv den elektroniske overvåking som fantes var meget kostbar. Det øst-tyske politiet (STASI) hadde for eksempel ansatt ca. 1/2 million hemmelige informanter, og 10.000 av disse var ansatt bare for å avlytte og avskrive telefonsamtaler. I løpet av 1980-tallet kom det nye former for elektronisk overvåking, med automatiserte avlyttingsmuligheter. I USA gikk utviklingen videre på 1990-tallet: Avslutningen av den kalde krigen førte til reduksjoner i militære kontrakter, noe som førte data- og elektronikkbransjen til nye markeder – hjemme og ute – med utstyr opprinnelig utviklet for det militære. Selskapene selger nå computersystemer og overvåkingsutstyr til de styrende på statlig og lokalt nivå, som bruker dem i rettshåndhevelsen, grensekontrollen og velferdsadministrasjonen. Regelmessig og rutinemessig masseovervåking av store deler av befolkningen, uten særlige formelle skranker, muliggjøres gjennom slike systemer og slikt utstyr, kombinert med videokameraer, teknikker for ansiktsgjenkjennelse og ID-kort (s. 16 i Wrights rapport).

Dette er smakebiter. Jeg skal gi noen konkrete eksempler på hvordan politiet nyttiggjør seg eller vil komme til å nyttiggjøre seg informasjonsteknologien.

Schengen

Først det såkalte *Schengensamarbeidet*, opp til i fjor formelt utenfor EU, nå innenfor. Innenfor Schengensamarbeidet er to omfattende registrerings- og overvåkingssystemer under utvikling. Det første går under navnet SIS – *Schengen informasjonssystem*. Artikkel 93 i Schengenkonvensjonen fra 1990 angir formålet:

> Formålet med Schengen-informasjonssystemet er, i samsvar med bestemmelsene i denne konvensjon, å opprettholde den offentlige orden og sikkerhet, herunder statens sikkerhet, og anvende bestemmelsene om persontrafikk i denne konvensjon på konvensjonspartenes territorium ved hjelp av opplysningene som formidles gjennom systemet.

Som en ser, er formålsbestemmelsen meget vid og omfattende. Den innbefatter *både* "den offentlige orden" og "statens sikkerhet". Noen nærmere presisering finnes ikke, hvilket betyr at omtrent alt er innbefattet. Artikkel 94 nr. 3 i Schengenkonvensjonen gir de grunnopplysninger som kan registreres om personer:

Fornavn, etternavn og eventuelle "aliasnavn"; særskilte objektive og uforanderlige fysiske kjennetegn; første bokstav i 2. fornavn; fødselsdato og sted; kjønn og nasjonalitet; om vedkommende er bevæpnet; om vedkommende formodes å være voldelig; grunnen for registreringen; samt tiltak som skal treffes. Grunnopplysningene danner altså en kombinasjon av objektive (kjønn) og vurderende (formodet voldelighet) informasjoner.

Men det er bare begynnelsen. Artikkel 94 nr. 1 fastsetter at opplysninger bare kan registreres når dette er nødvendig etter formålene i artiklene 95–100. Artikkel 95–99 gjelder personer, mens artikkel 100 gjelder gjenstander. Artikkel 95 gjelder personer som ønskes anholdt med sikte på utlevering, artikkel 96 gjelder uønskede utlendinger, artikkel 97 gjelder forsvundne personer eller personer som ikke kan ta vare på seg selv, artikkel 98 gjelder vitner (!), tiltalte eller personer som skal ha en dom forkynt, artikkel 99 gjelder personer som man ønsker å underkaste "diskret overvåking" (!) eller såkalt målrettet kontroll. Den franske originalteksten bruker betegnelsen "surveillance discrète", mens den offisielle norske oversettelsen bruker det forskjønnende ordet "observasjon" (den danske oversettelsen sier, ærligere, "diskret overvågning", den svenske "hemlig övervakning")[1]. Det dreier seg om registrering av opplysninger med henblikk på spaning.

Som ledd i diskret overvåking med hjemmel i artikkel 99 kan i sin tur forskjellige andre opplysninger innsamles og overføres til myndighetene i det land som har anmodet om diskret overvåking i en bestemt sak: at den aktuelle person eller kjøretøy er funnet, sted, tidspunkt eller grunn for kontrollen, reiserute og reisemål, ledsagere (!) og passasjerer (!), kjøretøy som er benyttet, medbrakte gjenstander, under hvilke omstendigheter personen eller kjøretøyet er observert.[2]

Artikkel 99 nr. 2 angir noen av betingelsene for bruk av diskret overvåking. De er delvis nokså presise, og delvis meget vage, og åpner for diskret overvåking av brede kategorier av personer. I Artikkel 99 nr. 2 a) heter det at melding kan foretas "når det foreligger konkrete holdepunkter for å anta at vedkommende person planlegger å begå eller begår et større antall og særdeles alvorlige straffbare handlinger". Bestemmelsen er forholdsvis presis. I Artikkel 99 nr. 2 b) heter det imidlertid at melding også kan foretas "når det ut fra en samlet vurdering av vedkommende person, særlig på grunnlag av tidligere begåtte straffbare handlinger, må antas at vedkommende også i framtiden vil begå særdeles alvorlige straffbare handlinger". Bestemmelsen er vag og åpen ("ut fra en samlet vurdering", "må antas at"), og dreier seg bare om mulige fremtidige, hypotetiske handlinger.[3]

Dessuten åpner artikkel 99 nr. 3 mulighet for diskret overvåking på grunnlag av politisk atferd. Det heter nemlig i artikkel 99 nr. 3 at "[m]elding kan også foretas med hjemmel i nasjonal rett på anmodning fra de instanser som har ansvaret for statens sikkerhet, når det foreligger konkrete holdepunkter for å

anta at opplysningene omhandlet i nr. 4 [som angir opplysningene som kan innsamles i forbindelse med diskret overvåking, TM] er nødvendige for å forebygge en alvorlig trussel fra vedkommende persons side eller andre alvorlige trusler mot statens indre eller ytre sikkerhet." "[I]nstanser som har ansvaret for statens sikkerhet" vil på godt norsk si Overvåkingspolitiet, og artikkel 99 nr. 3 inneholder ikke ett ord om at det skal dreie seg om kriminelle handlinger. Prosedyren som skal følges av "instanser som har ansvar for statens sikkerhet" når de ber om diskret overvåking, er angitt i en hemmelig såkalt "SIRENE-håndbok", som jeg kommer tilbake til.[4]

Som en ser, kan mange av opplysningene i systemet karakteriseres som vidtrekkende, mange av dem bygger på skjønn, og særlig i forbindelse med anmodninger i SIS om "diskret overvåking" ligger det mulighet for å opplyse til myndigheter i et annet land om en vid krets av personer (ledsagere, passasjerer) rundt den hovedperson man er interessert i. I diskret overvåking ligger det etter konvensjonen også mulighet for å overvåke på politisk grunnlag.

Schengen informasjonssystem har en sentral database i Strasbourg, og nasjonale SIS-baser i alle medlemsland. De nasjonale databasene skal ha identisk informasjon lagret, og denne informasjonen skal i sin tur være identisk med informasjonen som er lagret i Strasbourg. Informasjonen legges inn etter nasjonal lovgivning, men kan tas ut i alle medlemsland. I 1997 var tallet på "adgangspunkter" ("access points") ca. 48 700 i de ni stater som da hadde tilknytning. Tallet er hentet fra rapport av 25. september 1998 fra styringsgruppen i SIS.[5] Tallet er enormt, selv om det er noe uklart om det dreier seg om rett til utlevering av opplysninger eller direkte søk (eller begge deler). Allerede i 1994, før Schengen trådte i kraft, hadde hele 63 ulike politi- og tollmyndigheter, flere av dem overordnete og meget omfattende, adgang til å søke opplysninger med hjemmel i en eller flere av artiklene 95–100 i konvensjonen. Det fremgår av en note fra styringsgruppen i SIS av 17. juni 1994. Det samlede antallet lagrede opplysninger ("gespeicherten daten", oversatt til engelsk med "records" eller "record entries") i hele Schengenområdet var pr. 26. mars 1996 nesten 3,9 millioner.[6] Tyskland og Frankrike var de store brukerne. Det var lagret informasjoner om hundre tusenvis av personer. Den endelige lagringskapasiteten var den gang 9 millioner opplysninger. Tallet gikk opp for hvert år, fra 4,6 millioner i 1996 til 5,6 millioner i 1997 og hele 8,8 millioner i 1998. Disse tallene er basert på antall "record entries" (angående både personer og gjenstander) på *en enkelt dag* (for 1998: 5. mars), og speiler ikke antallet som er lagt til eller slettet i løpet av året.[7]

Systemet er altså meget stort, både målt ved mengden av personer og informasjoner som er lagret *og* i form av utbredelse og bruk gjennom Europa.

Til tross for at systemet et stort, står man foran utvidelser. Man har en rekke planer: Videreutvikling og teknisk oppdatering av den sentrale SIS-basen i Strasbourg, Nordens integrasjon i systemet, større kompatibilitet mellom SIS og andre europeiske registreringssystemer, mv.[8]

Det fantastiske omfanget av hele prosjektet er mer enn klart.

SIS er imidlertid bare det ene systemet for informasjonsutveksling i Schengen. Det andre samarbeidet kalles *SIRENE,* med det lange navnet *Supplément d'Information Requis a l'Entrée Nationale* (Supplementary Information Request at the National Entries). Den nasjonale registeransvarlige etat for Schengen informasjonssystem kalles SIRENE-kontor. Men SIRENE står også for noe mer. Det dreier seg om et teknisk støttesystem for bilateral og multilateral utveksling i første rekke av tilleggsinformasjon, mellom de nasjonale politimyndigheter i de ulike Schengenland, om personer og gjenstander registrert i SIS. Gjennom SIRENEs system kan politiet i ett medlemsland, som har arrestert en person som et annet land har registrert i SIS, kreve tilleggsinformasjon (som ikke finnes i SIS) fra det landet som har registrert personen i SIS. Dette samarbeidet, som har vokst fram ved siden av SIS, er langt mindre kjent, og det er ikke en gang nevnt i Schengenkonvensjonen. Det *er* imidlertid nevnt i utkast til konvensjon om Det europeiske informasjonssystem, EIS (som i dag er overflødig fordi Schengen nå formelt er inkorporert i EU og har overtatt funksjonene). Her fremgår det klart at SIRENE innlemmer og utveksler meget generell og særdeles vidtrekkende informasjon om personer. Det heter (mine uthevinger):

> I forbindelse med innlemmelse av et signalement eller med iverksettelse av en påfølgende handling, utveksler SIRENE-tjenestene, med skyldig hensyntaken til nærværende konvensjon og deres nasjonale lover, *de utfyllende opplysninger som er nødvendige* for å identifisere signaliserte personer eller gjenstander såvel som *andre opplysninger og dokumenter av viktighet* for fortsettelsen av aksjonen som er foretatt.

Opplysningene legges inn etter nasjonal lovgivning, men i praksis vil det si opplysninger som fra før er registrert i politiets nasjonale arbeidsregistre,[9] og som inneholder hele arsenaler av sensitive opplysninger.[10] Det er dokumentert at SIS og SIRENE utgjør to forskjellige "trafikk"-systemer eller "nett".[11] SIS omfatter tross alt bare begrensede, og for det meste såkalte "standardiserte", opplysninger. De nasjonale SIRENE-enheter, som for øvrig også administrerer SIS, behandler derimot omfattende ikke-standardisert informasjon, "myke" data (et vanlig begrep i interne håndbøker for politiet) også om ikke mistenkte personer. "[D]e utfyllende opplysninger som er nødvendige", og "andre opplysninger og dokumenter av viktighet", er høyst upresise, omfattende begreper og uttrykksmåter, som kan innbefatte omtrent alt. Det samme er understreket fra SIRENE-medarbeidere selv. Sjefen for det portugisiske SIRENE-kontoret uttalte følgende til norsk TV (NRK1) 10. mars 1997:

> Det er konvensjonen som sier hvem som har tilgang til systemet. Men generelt har politiet det. De er jo på flyplasser, i havnene, og kan avlytte mobiltelefoner. Det gjør at de har tilgang til en masse informasjon hele tiden. De trenger ikke å hente fakser. Dette er et hurtig system. Det er oppdatert. Det er en masse informasjon. Og det er naturlig at effektiviteten er mye bedre enn i det tradisjonelle Interpol-systemet.

Politiet avlytter mobiltelefoner, og, i følge den portugisiske sjefen, kommuniseres resultatene mellom SIRENE-kontorene. SIRENE-samarbeidet kan sies å være en formalisering og legitimering, og derved en meget betydelig styrkelse, av utvekslingen av informasjon mellom politietater i forskjellige land, som har pågått og økt jevnt over de siste par tiår.

Kommunikasjonsaspektet er overordnet i SIRENE-sammenheng. Det er utarbeidet en stor håndbok for SIRENE. Håndboken er hemmelig, men flere deler av den, og oppsummeringer, er allerede offentlig tilgjengelig.[12] Tidsskriftet *Fortress Europe?* har gjennomgått SIRENE-håndboken i desember/januarnummeret 1996/97. På grunnlag av håndboken oppsummerer tidskriftet SIRENEs omfattende virksomhet slik, en oppsummering jeg etter egen lesning av håndboken kan slutte meg til:

> SIRENE kan best beskrives som en kompleks, nettverkspreget struktur for bilateralt og multilateralt politi- og sikkerhetssamarbeid mellom Schengenland, innbefattet sentrale nasjonale kontorer og et sofistikert databasert informasjonssystem, som gjør det mulig å utveksle "tilleggsinformasjon" om personer og gjenstander før en rapport lagres i SIS og etter et treff (positiv søk) i SIS. Sammenliknet med mengden og følsomheten av informasjon som kan bli lagret og utvekslet av SIRENE-kontorene, er SIS i virkeligheten lite annet enn et indekssystem.

SIRENE kommuniserer som sagt bilateralt og multilateralt opplysninger som *supplerer* informasjonen i SIS. Dette slås klinkende klart fast i innledningen til håndboken, slik (s. 11; alle sitater/oppsummeringer fra håndboken nedenfor er også sitert eller oppsummert i *Fortress Europe?,* desember 1996/januar 1997):

> S.I.S. er sammensat af to dele: et centralt system og flere nationale informationssystemer (ét i hvert land). Systemet fungerer på den måde, at data ikke kan udveksles direkte mellem de nationale informationssystemer, men udelukkende via det centrale system (C.S.I.S.).
>
> De supplerende oplysninger, som er nødvendige for anvendelsen af visse af Konventionens bestemmelser og de oplysninger, som er nødvendige for at Schengen-informationssystemet kan fungere, skal dog kunne udveksles bi- eller multinationalt mellem de kontraherende parter.
>
> Hver national del af Schengen-informationssystemet (N.S.I.S.) skal således, for at kunne imødekomme de funktionskrav, som forundersøgelsen og Konventionen har fastlagt, også indeholde SIRENE-strukturen, som er absolut nødvendig for anvendelsen af edb i systemet.
>
> Enhver supplerende oplysning påkrævet ved indrejse i et land vil gå gennem denne tekniske og driftsmæssige støttefunktion.

Det er imidlertid meget viktig å være klar over at bruken av SIRENE-systemet *ikke er begrenset til tilleggsinformasjon til opplysninger som er lagret i SIS.* Håndboken fastslår nemlig under 3.2.1. (s. 39):

> Samarbejdet mellem de kontraherende parter og politiets sagkyndige kan ikke kun begrænses til brugen af oplysningerne i Schengen-informationssystemet. Opdagelsen af en indbe-

retning kan føre til afsløringen at en overtrædelse eller en alvorlig trussel mod den offentlige orden og sikkerhed, lige som det kan være nødvendigt at foretage en præcis identifisering av en person eller genstand. Udveksling af oplysninger i form af f.eks. fotografier eller fingeraftryk kan vise sig at være altafgørende. Artikkel 39 og 46 tillader disse fremgangsmåder. Disse informationsudvekslinger skal overholde bestemmelserne angivet i Konventionens Afsnit VI.

Artikkel 39 og 46, som det her henvises til, gjelder ikke SIS, men henholdsvis gjensidig bistand mellom konvensjonspartenes politimyndigheter for å forebygge og oppklare straffbare handlinger (artikkel 39), og uoppfordret oversendelse mellom konvensjonspartene av opplysninger som kan ha betydning "i forbindelse med forfølgning av fremtidige lovovertredelser og forebygging av straffbare handlinger eller [NB, eller!] handlinger som utgjør en trussel mot offentlig orden og sikkerhet" (artikkel 46 nr. 1). Ordet *eller*, som også brukes i originaltekstene (tysk og fransk) til konvensjonen, er av største betydning: Man kan også oversende opplysninger som *ikke* har med straffbare handlinger å gjøre. Under 3.2.2. i håndboken påpekes det at SIRENE-kontorene tilbyr "en operationel struktur, som i visse tilfælde kan vise sig at være meget nyttig".

Anvendelsesområdet er altså særdeles vidt. SIRENE er et komplekst informasjonssamarbeid om vidtrekkende og uavgrensede opplysninger som utdyper SIS, men som også lever sitt eget liv helt uavhengig av SIS.

Til slutt om Schengen: Det sies at Schengensamarbeidet først og fremst handler om bekjempelse av kriminalitet. La meg slå fast at det gjør samarbeidet ikke. Rapport etter rapport etter rapport fra Schengen selv – både når det gjelder Schengen informasjonssystem og på SIRENE-nivå – viser klart at samarbeidet først og fremst handler om *kontroll med uønskede fremmede.* Det er migrasjonen mot Europas yttergrense som først og fremst skal overvåkes, og det er uønskede fremmede som er kommet inn som skal kastes ut. Derfor kalles samarbeidet av og til for et samarbeid om byggingen av "den europeiske festning".

Det sies at vi som er innenfor festningen til gjengjeld vil ha reise- og passfrihet gjennom Europa. Men vi vet at flere land har (delvis mobile og mer overraskende) kontroller i soner innenfor sine egne grenser (se nærmere Mathiesen 1997 s. 31–32), rent bortsett fra at man må kunne identifisere seg når man reiser.

Europol

Så litt om *Europol.* Europol er selve kjernen i EUs politiarbeid. Schengen handler som sagt (i motsetning til hva politikerne har forsøkt å fortelle oss) ikke om kriminalitetsbekjempelse, men først og fremst om utestengning av fremmede ved den felles ytre Schengengrensen. Europol, derimot, handler om alvorlig, grenseoverskridende organisert kriminalitet. Til gjengjeld er personvernsproblemene, som allerede er av avgjørende betydning i Schengen, så formidable i Europol at man overskrider en ny kvalitativ grense.

Europols datasystemer (The Europol Computer Systems, TECS) er Europols hjerte og hjerne. Disse formidable systemene ble avspist med 7 linjer i den norske stortingsmeldingen om saken fra i fjor (St. meld. nr. 18 for 1999–2000). Det har tre hovedregistre. For det første et *sentralt register* som skal inneholde standardiserte data, innbefattet persondata, om personer dømt eller mistenkt for å ha begått eller tatt del i lovbrudd innen Europols arbeidsområde, samt mulige fremtidige lovovertredere innen området. Informasjonssystemet er altså klart innrettet mot lite avgrensede mulige fremtidige lovstridige handlinger, en meget bred og diffus kategori. For det andre *analyseregistrene.* Det er spesielle midlertidige registre for analyse av særskilte aktivitetsområder, med omfattende data – også "myke" data – om personer registrert i informasjonssystemet, dessuten om mulige vitner (!), ofre (!) eller personer som det er grunn til å tro kan bli ofre (!), kontakter og forbindelser (!), samt personer som kan gi informasjon om kriminalsakene som er aktuelle. I sannhet en meget vid ring av personer rundt – og løst knyttet til – dømte eller mistenkte personer. Vi ser allerede her hvordan personvernproblemene tårner seg opp. Og for det tredje *indekssystemet.* Der vil en ha nøkkelord angående informasjoner registrert i analyseregistrene, slik at det blir mulig å finne ut om og hvor data om nøkkelordene finnes. Registrene skal være i gang i 2001.

De typer nærmere personopplysninger som kan lagres i analyseregistrene er ikke angitt i konvensjonen, bare i såkalte "iverksettelsesregler for analyseregistre", som er gitt med hjemmel i konvensjonen. Iverksettelsesreglene skal i utgangspunktet ikke godkjennes av parlamentene, bare vedtas ved enstemmighet på ministerplan (Europolkonvensjonens artikkel 10 nr. 1).

Som eksempel på hva slags personopplysninger man ønsker å kunne lagre i analyseregistrene, nevner jeg at det i 1996 kom på bordet et forslag fra en arbeidsgruppe som gikk ut på at det skulle som tilleggsopplysninger være mulig å registrere høyst personlige og intime opplysninger om personer: Rasemessig opprinnelse, religiøs eller annen tro, seksualliv, politiske meninger m.v. Det skulle være forbudt å samle opplysninger *bare* på grunnlag av at de hadde med slike forhold å gjøre. Det betyr at det *skulle* være mulig å samle opplysninger om slike forhold når de ikke sto alene. Forslaget ble kritisert, bl.a. i EU-parlamentet, og gikk gjennom en lengre prosess der betingelsene for lagring ble noe innsnevret. *Men slike intime personopplysninger skal fremdeles kunne registreres* dersom opplysningene "er betraktet som strengt nødvendige for formålet med den aktuelle analysearbeidsfilen". Når det gjelder ofre eller mulige ofre, mulige vitner og informanter, skal slike data bare kunne lagres etter at spesielle grunner er angitt og etter uttrykkelig krav fra to eller flere medlemsstater. I praksis er disse begrensningene meget langt fra stramme. Disse helt avgjørende registreringsmuligheter er for øvrig ikke nevnt med et eneste ord i den før nevnte norske stortingsmeldingen.

Men stenger ikke EUs personverndirektiv for slikt? EUs personverndirektiv

gjør eksplisitt unntak bl.a. for "statens virksomheter på det strafferettslige område" (artikkel 3.2). Den ovennevnte registreringen av sensitive opplysninger rammes ikke av personverndirektivet.[13]

Iverksettelsesreglene for analyseregistrene tillater for øvrig innsamling, lagring og utnyttelse av hele 53 (!) typer personopplysninger om personer registrert i informasjonssystemet. De 53 typene personopplysninger er gruppert i 10 kategorier, f.eks. personlige detaljer (14 typer opplysninger), fysisk utseende (2 typer opplysninger), identifikasjon og dokumenter (5 typer opplysninger, innbefattet DNA-opplysninger, dog "utenom opplysninger som karakteriserer personligheten"), yrke og andre kvalifikasjoner (5 typer opplysninger), økonomiske og finansielle opplysninger (8 typer opplysninger) "atferdsdata" ("behavioural data"; 8 typer opplysninger som bl.a. innbefatter "livsstil og vaner"), m.m.

Dessuten er en ytterligere kategori gitt navnet "Andre databaser hvor opplysninger om personen er lagret". Dette gjelder databaser under Europol, politi- og tollmyndigheter, andre håndhevende myndigheter, internasjonale organisasjoner (!), samt offentlige (!) og private (!) institusjoner.

Det fremgår at de ovennevnte typene opplysninger ikke bare kan nyttes om personer som er mistenkt for å ha begått eller tatt del i en kriminell handling under Europols arbeidsområde (en meget vag og vid kategori i seg selv), men at de også kan nyttes om vitner, ofre og mulige fremtidige ofre, kontakter og forbindelser samt informanter.

Europolkonvensjonen trådte i kraft 1. oktober 1998, og Europol ble operativ 1. juli 1999. Ratifiseringen og ikrafttredelsen skjedde på tross av tilbakevendende sterk kritikk på personvern- og rettssikkerhetsgrunnlag. Selv *medarbeidere innen Europol* har gitt uttrykk for kritikk og tvil. Videre rettet tyske tilsynsmyndigheter på delstatsnivå i oktober 1997 heftig kritikk mot rettssikkerheten i Europol. Kritikken kom fram på en konferanse for delstatstilsynsmyndighetene i Bamberg i 1997. Likeledes har Det tyske dommerforbund og Det tyske riksadvokatembete fremsatt kritikk.Visserlig skal en felles kontrollmyndighet etableres. Organet får imidlertid ikke noen reell makt. Det fremgår av det utkast til forretningsorden for kontrollmyndigheten som ble behandlet på Ministerrådsmøtet for justis- og innenrikssaker 24. september 1998, og igjen utkastet som ble behandlet på Rådsmøtet 3.-4. desember 1998. I referatet fra det sistnevnte møtet brukes uforpliktende uttrykk som "gjennomgå" og "holde oppsyn med" ("review" og "monitor") Europols aktiviteter for så vidt gjelder individers rettigheter og adgangen til å overføre data som har opprinnelse i Europol.

Men dette er ikke slutten. Det heter i en protokoll som også er ratifisert i alle land at alle Europolansatte får "immunitet fra rettslige skritt av enhver art med hensyn til ord uttalt eller skrevet, og med hensyn til handlinger utøvd av dem, i utførelsen av deres offisielle funksjoner". Riktignok kan Europols direktør tilsidesette immuniteten "i tilfeller der immunitet ville hindre at rettferdighet skjer fyldest og kan bli tilsidesatt uten at Europols interesser blir skadet." Men dette er jo det samme som å la den velkjente bukken passe havresekken.

Protokollen om immunitet ble ansett for å være av meget stor betydning i EUs besluttende organer, og er et langt skritt mot etablering av "et Europas FBI med operativ politimyndighet", for å bruke den norske stortingsmeldingens ord om hva man tilsynelatende ikke tar sikte på.

Andre systemer

Europol er planlagt med sikte på vidtrekkende integrasjon f.eks. med Schengen informasjonssystem. I tillegg står Europol foran integrasjon med et omfattende fingeravtrykksystem beregnet på asylsøkere i Europa, med tvungen registrering med fingeravtrykk og andre data av alle asylsøkere over 14 år i alle EUs medlemsland (Eurodac; jeg vet ikke hvor mange hundre tusen mennesker dette vil dreie seg om),[14] og utvikling av et globalt system for avlytting av telefon, e-mail, fax, mobiltelefon m.v. (i de såkalte ENFOPOL-dokumentene, avslørt av Tidsskriftet *Telepolis*). Med ENFOPOL-dokumentenes skisser og planer når overvåkingen av telekommunikasjoner helt fantastiske proporsjoner. Jeg skal til slutt si noen få ord om ENFOPOL-dokumentene, for å få fram nettopp det fantastiske i dette.

Planleggingen skjer innenfor EUs arbeidsgruppe for politisamarbeid (EU Police Cooperation Working Party). Begynnelsen var et møte i 1993 mellom representanter for en rekke stater i byen Quantico i Virginia, der FBI-akademiet holder til. Der dannet man et såkalt "International Law Enforcement Telecommunications Seminar", ILETS (se nærmere Campbell 1999 a). Det hele er nokså uoversiktelig for offentligheten, men arbeidet videre gikk gjennom flere ledd, bl.a. et EU-memorandum om lovlig teleavlytting i 1995 som også Norge sluttet seg til, og fram til arbeidet i EU Police Coperation Working Party. Arbeidsgruppen, som også har andre oppgaver enn å planlegge avlytting av telekommunikasjoner, er omgitt av mye hemmelighold,[15] men tidsskriftet *Telepolis* har avdekket en del av gjøremålene (http://www.telepolis.de/tp/deutsch/special/enfo/6329/1.html).

Man planlegger et system for avlytting av enhver form for telekommunikasjon – data, enten den er kryptert eller ikke, ordinære mobiltelefoner, mobiltelefoner via satellitt så vel som Internettkommunikasjon. Dokumentene som er avdekket har fått betegnelsen "ENFOPOL-dokumentene". Jeg har lest mange av dem selv. Som det heter i en oppsummering av ENFOPOL-dokumentene av Armin Medosch datert 30. november 1998 (Medosch 1998) på ovennevnte Internettadresse:

> Hvis disse planene blir satt i verk, vil [man] være i stand til å avlytte nesten enhver kommunikasjonsform, og ikke la noe forbli udekket. For å unngå rettslige problemer hvis målene for overvåking flytter seg raskt fra et land til et annet og også for å sikre de avlyttede opplysningene, ser [man] den sentrale jordbaserte hovedstasjonen for Iridium i Italia som et ideelt sted for avlytting av telekommunikasjonstrafikk. Men også store betalingssentraler [clearing houses] som håndterer oppkrav for internasjonale telefoner nevnes som potensielle kilder for den slags informasjon som europeiske politistyrker er interessert i.

I øyeblikket er innholdet i ENFOPOL-dokumentene om nær sagt altomfattende avlytting av alle slags telekommunikasjonsmidler ikke realiteter, men på forslagsstadiet. Planene har også vært utsatt for sterk kritikk, bl.a. av internettleverandører som – for så vidt som det gjelder Internett – ser dem som både prinsipielt problematiske og enormt kostbare (Campbell 1998). Etter at de offisielle dokumentene lekket ut gjennom *Telepolis* ble planene også tatt opp kritisk i EU-parlamentet av irske Patricia McKenna. Men planene har nådd toppnivået i EU-strukturen: De ble tydeligvis drøftet for eksempel på møtet 27.–28. mai 1999 i Ministerrådet for justis- og innenrikssaker, hvor de ble koblet til en diskusjon av utkastet til konvensjon om rettslig assistanse i kriminalsaker. I referatet fra møtet, tatt ned fra Internett, sies det eksplisitt at "Rådet diskuterte nok en gang problemet med avlytting av telekommunikasjoner, som dekker tradisjonell telefoni, GSM [mobiltelefoni, min anmrk.] og internasjonale satellittbaserte nettverk, som er et av de siste – men særlig vanskelige – åpne spørsmål knyttet til dette konvensjonsutkastet." Et meget viktig spørsmål gjelder "fjernkontroll" eller "remote control". Under "fjernkontroll" kan en medlemsstat som ønsker å foreta en avlytting av et mål på dens territorium gjøre det gjennom en nasjonal tjeneste for et satelittnettverk selv om bakkestasjon for nettverket er lokalisert i en annen medlemsstat, og uten teknisk assistanse fra bakkestasjonen. Konvensjonsutkastet fastslår at medlemsstaten som har bakkestasjonen ikke skal ha noen rolle i avlyttingen fordi målet for selve avlyttingen ikke er på dens territorium. Med en slik ordning er avlyttingen av satellitter virkelig brutt løs. Italia er den første medlemsstaten som har en slik bakkestasjon i gang, for satellittnettverket Iridium, og spørsmålet er sensitivt. Meget sterke krefter går inn for de vidtgående fullmaktene på avlytting.

Er så slike planer, i hvert fall når det gjelder masseovervåking av satellittbasert kommunikasjon, teknisk gjennomførbare? Det såkalte Echelon-samarbeidet, som *er* en realitet, viser at så er tilfelle.

Et parallelt overvåkingssystem, som dekker flere stater i og utenfor EU, er blitt kalt Echelonsystemet. De overenskomster, planer og forslag om overvåking av telekommunikasjon fra FBI-seminaret i Quantico i 1993 gjennom ILETS og memorandumet i 1995 til de såkalte ENFOPOL-dokumentene, kan samlende betegnes som *EU-FBI-systemet,* som tar sikte på å betjene politi- og justisvesenet. *Echelonsystemet,* på den andre siden, betjener det militære etterretningssystemet. Echelon er altså et regulært spionsystem. Men til forskjell fra mange av de elektroniske spionsystemene som ble utviklet under den kalde krigen, er Echelon tydeligvis like mye beregnet for ikke-militære mål – regjeringer, organisasjoner og forretningsselskaper verden over. USA, Storbritannia, Canada, New Zealand og Australia er hoveddeltakere, med USA som den mektigste partneren. Den før nevnte rapporten til Europaparlamentet av Steve Wright (Wright 1998), beskriver Echelons virksomhet bl.a. med følgende ord (januarutgaven, s. 19–20; se også Hager 1996):

> Moderne teknologi er så godt som gjennomsiktig når det gjelder det avanserte avlyttingsutstyret som kan brukes for å overvåke. ... Innen Europa blir all e-mail, telefon- og telefaxkommunikasjon rutinemessig avlyttet av USAs National Security Agency, idet man overfører all målinformasjon fra det europeiske fastland via den strategiske sentral i London og så ved satellitt til Fort Meade i Maryland [NSAs hovedkvarter, lokalisert mellom Baltimore og Washington D.C.,TM] via den avgjørende sentral ved Menwith Hill i North York Moors i Storbritannia.... Echelonsystemet virker ved udiskriminerende å avlytte meget store mengder kommunikasjon, for så å kryste ut det som er verdifullt ved å bruke kunstige intelligensmidler som Memex for å finne nøkkelord. Fem nasjoner deler resultatene. Hvert av de fem sentrene forsyner de andre fire med 'ordbøker' med nøkkelord.

Undersjøiske telekabler er ikke lette å avlytte. Men det er mulig, og dessuten kan de lettere avlyttes når de går ned i eller opp av vannet. Det viktigste er imidlertid at satelittene er fremtiden. Nylig ble det opprettet en egen hjemmeside på Internett med løpende opplysninger om Echelon, så det som var svært så hemmelig går det nå an å følge noe med i (http://www.altavista.com/cgi-bin/query?q=echelon+nsa&pg=q&qe).
Jeg tillater meg også å vise til min egen bok, *Siste ord er ikke sagt. Schengen og globaliseringen av kontroll,* som kom tidligere i år (Mathiesen 2000, se også Mathiesen 1997) samt Duncan Campbells eksepsjonelle *Interception Capabilities 2000,* rapport til generaldirektøren for forskning under Europaparlamentet i april 1999 (Campbell 1999 b).

Fire punkter

Fire punkter til slutt: For det første, og for å gjenta: Flere av systemene er ikke innrettet først og fremst mot alvorlig grenseoverskridende kriminalitet. Dette til tross for hva politikerne sier. Schengen er primært innrettet mot grense- og fremmedkontroll. EURODAC likeså. Noe kriminalitet kan nok komme inn, men det er først og fremst "de uønskede fremmede" som er i fokus.

For det andre: De systemene som *er* innrettet mot alvorlig grenseoverskridende kriminalitet – som Europol – representerer til gjengjeld formidable personvernproblemer. Dessuten er det lite som overbeviser meg om at de er effektive midler mot den "organiserte kriminaliteten". "Kriminaliteten på grasrota" tar andre veier enn det registrene tilsier. Rent bortsett fra at den "organiserte kriminaliteten", etter de forskningserfaringer vi har, synes å være urealistisk overdrevet, inntil det paniske, i mediene og blant politikerne (se Christie 1999, Bäckman 1998, Bäckman 1999; se også Mathiesen 2000, note 84 s. 85–87).

For det tredje: Flere av systemene har regler om datakvalitet og personvern. La det være klart sagt. Schengen informasjonssystem (men ikke SIRENE) og Europol har det, og man har arbeidet mye med dem. Det er bare det, at reglene lett gjennomhulles av praktiske forhold: Kontrollorganene er svake. Les hva den norske datatilsynssjefen, Georg Apenes, har sagt og skrevet om kontrollorganet i Schengen, der han er med som en av to norske representanter (se nærmere Mathiesen 2000, s. 56–60). Politikulturene, og dermed regeltolkningen, gjen-

nom Europa, er meget varierende. Teknologiutviklingen er gallopperende. Spørsmålet om dagens IT-utvikling i det hele tatt *egner seg* for regulering gjennom den typen lover og regler som vi har, er rettssosiologisk sett meget interessant. Og aksesspunktene og aksesspersonene er mangefoldige – som sagt 48 000 aksesspunkter i Schengen informasjonssystem. Systemet lekker rett som det er som en sil. I november 1997 ble hele bunker av utskrifter fra Schengen informasjonssystem funnet – av alle steder – på en togstasjon i Belgia. Jeg vet ikke om de lå på en benk eller en søppelkasse. Utskrifter ble også funnet hjemme i leiligheten til en belgisk medarbeider. Dette er antakelig toppen av isfjellet. Og, viktigst, bare små dreininger i den politiske vind kan gjøre systemene farligere enn noe vi har sett tidligere. Haiders parti har i dag regjeringsmakt i Østerrike. Under 2. verdenskrig brukte de tyske okkupantene i Norge Statistisk Sentralbyrås dissenterregister og Telegrafverkets radiolisensregister for å finne fram til jøder i riket, og utrydde dem (Søbye 1998). Og det var tungvindte, manuelle registre. I vår tid er det bare spørsmål om å trykke på knapper.

For det fjerde og til slutt: Vi ser allerede klare tegn til, og må forvente, koblinger mellom de systemene jeg kortfattet har risset opp. For eksempel foreslo High Level Group on Organized Crime allerede 9. april 1997 at Europol skulle få tilgang til informasjon lagret i Schengen informasjonssystem. Europol-konvensjonen åpner for vidtrekkende samarbeid og integrasjon med andre systemer. Man diskuterer om dette skal innebære tilgang når man ber om opplysninger, eller direkte søk. Et mer eller mindre integrert, mer eller mindre globalisert registrerings og overvåkingssystem reiser seg i horisonten, med en farlig indre dynamikk skapt av begeistrede teknikere og politifolk som verken politikere, lekfolk eller medier har innsikt i. Politikerne på høyt nivå vet knapt hva de vedtar. Lekfolk tror at informasjonsteknologien bare er et gode. Og mediene er ikke engasjert, fordi det hele er for komplisert og dermed ikke nyhets-verdig. Systemene får lov til å utvikle seg uten overvåking.

Det er på høy tid at *kriminalister* tar det som avtegner seg i horisonten alvorlig.

HENVISNINGER:

Ackroyd, Carol m.fl.: *The Technology of Political Control.* Harmondsworth/New York: Penguin (Pelican Books) 1977.

Bäckman, Johan: "Russia's Organised Crime: From Problems in the Structures of Thinking towards New Fields for Western Criminology". I *Scandinavian Studies in Criminology,* Bind 15, Oslo: Pax Forlag 1998, s. 135–167.

Bäckman, Johan: "Inflasjonen i kriminalitet i Russland". *Nordisk Øst-forum* 13. årg., nr. 1 1999, s. 35–39.

Campbell, Duncan: "ENFOPOL Plans Provoke Strong Opposition". *Telepolis* 31. desember 1998 (http:// www.heise.de/tp/english/special/enfo6398/l.html).

Campbell, Duncan: "Special Investigation: ILETS and the ENFOPOL 98 Affair". *Telepolis* 29. april 1999 a.

Campbell, Duncan: *Interception Capabilities.* Report to the Director General for Research of the European Parliament. Edinburgh 1999 b.

Christie. Nils: "En høyst nødvendig mafia". *Nordisk Øst-forum* 13. årg., nr. 1. 1999, s. 25–33.
Hager, Nicky: *Secret Power: New Zealand's Role in the International Spy Network.* Nelson, New Zealand: Craig Potton Publishing 1996.
Mathiesen, Thomas: *Schengen. Politisamarbeid, overvåking og rettssikkerhet i Europa.* Oslo: Spartacus 1997.
Mathiesen, Thomas: *Industrisamfunn eller informasjonssamfunn? Innspill til belysning av den høymoderne tid.* Oslo: Pax Forlag 1999.
Mathiesen, Thomas: *Siste ord er ikke sagt. Schengen og globaliseringen av kontroll.* Oslo: Pax Forlag 2000.
Medosch, Armin: "The European Secret Service Union". *Telepolis* 30. november 1998.
Søbye, Espen: "Jødeforfølgelsene under den annen verdenskrig: Et mørkt kapittel i statistikkens historie?". *Samfunnsspeilet,* 12 årg., nr. 4 1998, s. 2–17.
Wright, Steve: *An Appraisal of Technologies of Political Control. Final Report.* European Parliament, Scientific and Technological Options Assessment, 6. januar 1998; revidert rapport september 1998.
Min artikkel bygger for øvrig på en omfattende litteratur (se nærmere Mathiesen 2000) samt en stor mengde originaldokumenter.

Noter:

[1] Den norske SIS-loven, som implementerer konvensjonens bestemmelser i Norge, benytter også det forskjønnende uttrykket "observasjon", se først Ot.prp. nr. 56 (1998-99), § 8 i forslag til lov om SIS, fulgt opp av Justiskomite, Odelsting og Lagting våren 1999; se videre lov om Schengen informasjonssystem (SIS) av 16. juli 1999 nr. 66. På det tidspunkt hadde Norge en "sentrumsregjering". Man kunne forventet at en regjering utgått av partier som opprinnelig sa nei til Schengen i hvert fall hadde beholdt den korrekte betegnelsen "diskret overvåking", for å sette fram i klartekst hva det dreiet seg om. Antakelig ville det ha blitt forandret av Stortingets flertall, men regjeringen hadde da i det minste gjort sitt. Men nei, regjeringen gjorde ikke sitt. Men så var jo regjeringens forslag allment sett forskjønnende.

[2] Den norske SIS-loven nevner ikke "ledsagere", bare "passasjerer", se Ot.prp. nr. 56 (1998-99) § 8.2 i forslag til lov om SIS, fulgt opp av Justiskomite, Odelsting og Lagting våren 1999; se lov om Schengen informasjonssystem (SIS) av 16. juli 1999 nr. 66. Tanken er vel at "ledsagere" er innbefattet, og det ser penere ut. Den norske formuleringen vil ikke utgjøre noen realitetsforskjell.

[3] Samme formuleringer er brukt i forslaget til norsk SIS-lov, se § 8 nr. 1 a) og b) i Ot. prp. nr. 56 (1998-99), fulgt opp av Justiskomite, Odelsting og Lagting våren 1999; se lov om Schengen informasjonssystem (SIS) av 16. juli 1999 nr. 66.

[4] Med ett unntak gjenfinnes formuleringene i forslaget til norsk SIS-lov § 8 nr. 2, fulgt opp av Odelsting og Lagting våren 1999; se lov om Schengen informasjonssystem (SIS) av 16. juli 1999 nr. 66. Det heter der at registrering av opplysninger kan foretas når det foreligger konkrete holdepunkter for å anta at registreringen "er nødvendig for å forebygge en alvorlig trussel fra vedkommende persons side eller andre alvorlige trusler mot statens indre eller ytre sikkerhet". Unntaket er at det ikke finnes noen referanse i bestemmelsen til "de instanser som har ansvaret for statens sikkerhet", eller Overvåkingspolitiet. Formuleringen er heller ikke nevnt i merkadene til bestemmelsen (Ot.prp. nr. 56 (1998-99), s. 2), bare i beskrivelsen av hva som står i konvensjonen (s. 54). Grunnen til utelatelsen kan være at det norske overvåkingspolitiet ikke vurderer SIS som særlig nyttig, all den stund det er et åpent system der mange instanser kan hente ut informasjon (proposisjonens s. 68). Uansett vil instanser med ansvar for statens sikkerhet i *andre* Schengenstater kunne se det annerledes, og på grunnlag av konvensjonen og gjennom de konkrete prosedyrene angitt i SIRENE-håndboken henvende seg til eller til og med kreve av det norske Overvåkingspolitiet at opplysninger skal formidles. Slikt press kan i praksis være meget vanskelig å motstå. Utelatelsen av "de instanser som har ansvaret for statens sikkerhet" gir et mye mindre farlig og mye mindre politisk preg til loven enn konvensjonen borger for.

[5] Kilde for opplysningen: Statewatch European Monitor, Bind 1 nr. 1, 1998, s. 30, med *fulltekst gjengivelse* av rapport av 25. september 1998 fra Styringsgruppen for SIS. Slik kilden ordlegger seg, er det mest nærliggende at det her er snakk om det som i norsk terminologi omtales som "tilgang" på opplysninger, dvs. direkte søk i systemet, og ikke det som på norsk betegnes som "utlevering" av opplysninger, dvs. ikke direkte søk (i konvensjonen kalles dette henholdsvis for "rett til direkte søk" og "tilgang"). Selv om det skulle være en viss sammenblanding her, er tallet enormt. Det er ikke nevnt i Ot.prp. nr. 56 (1998-99) til tross for at det finnes (og fantes da proposisjonen ble skrevet) i helt offisielle kilder. Unnlatelsen kan ikke ha noe å gjøre med forsøk på å begrense Schengenkonvensjonens farlige sider. Det er en forskjønning som tildekker noe av det farligste i Schengensamarbeidet - muligheten for enorm spredning av personopplysninger.

Jeg tilføyer at i min behandling står "tilgang" for utlevering av opplysninger, mens betegnelsen "søk" dekker direkte adgang til et informasjonssystem.

[6] Kilde: Årsmelding fra Sentralgruppen i Schengen, 26. mars 1996.

[7] Kilde: Årsmelding fra Schengen for 1997; referert i *Statewatch* mai/august 1998, s. 27; tallet for 1998 referert i *Statewatch* mai/august 1999, s. 22. Tallet for 1998 innbefattet drøyt 1,2 millioner lagrede personopplysninger og 7,4 millioner opplysninger om gjenstander. På grunn av et relativt stort antall personer innenfor den såkalte "aliasgruppen", dvs. personer som har en falsk tilleggsidentitet, gjelder "bare" 795 000 av de 1,2 millioner lagrede personopplysningene virkelige personer. Tallet er sannelig stort nok. Nesten 5,3 - nær 72 % - av de 7,4 millioner opplysninger om gjenstander gjelder tapte eller stjålne identifikasjonspapirer. Bare ca. 15 % av opplysningene om gjenstander gjelder biler, og andre gjenstander - banksedler, våpen mv. - viser enda mindre andeler (2-3 % gjelder våpen). Jeg kommer senere tilbake til den hovedvekt som det i Schengen legges på uønskede fremmede, identitetskontroll mv. snarere enn kriminalitet.

Det er slettingsfrister for opplysninger i SIS. Av de tilgjengelige statistiske opplysningene ser det ikke ut til at disse er blitt overholdt til punkt og prikke. Den største "slettingsoperasjonen" fant sted i første halvår 1997. I følge en rapport fra det tyske SIRENE-kontoret slettet Tyskland 207 000 opplysninger som var lagret i medhold av artikkel 96, om uønskede fremmede, i løpet av denne seks måneders perioden. Det var nesten halvparten av de tyske artikkel 96-opplysningene i systemet den gangen. Opplysningene var blitt tatt over fra det tyske søkesystemet INPOL, og hadde vært i INPOL før 1994, og lastet over i SIS da SIS startet 26. mars 1995, slik at de samlet hadde vært lagret lengre enn treårsgrensen som Schengenreglene krever for slike opplysninger (kilde: *Statewatch* mai/august 1999, s. 24).

[8] Kilde: Arbeidsprogram for det østerrikske formannskap i Schengen annet halvår 1997, s. 8; se også *Informationsblatt: Eine Mitarbeiterinformation des Bundesministeriums für Inneres* nr. 1, september 1997, s. 3; se videre Referat fra møte 7. oktober 1997 i Schengens eksekutivkomite under det østerrikske formannskap.

[9] Jfr., for Norges vedkommende, Ot. prp. nr. 56 (1998-99) s. 123-124 og SIS-lovens § 11.

[10] Se Mathiesen 2000 s. 47-50.

[11] Kilde: Arbeidsdokument fra Det belgiske formannskapet i Schengen og Benelux av 29. mai 1995.

[12] Se bl.a. *Fortress Europe?* desember 1996/januar 1997, samt Mathiesen 1997 og 2000. Det er også opplyst at noen har lagt håndboken ut på Internett (kilde: den danske justismininister Frank Jensen på møte i Rådet for Europæisk Politik 4. februar 1999). Hemmeligholdet er i medhold av Schengen eksekutivkomites beslutning av 14. desember 1993, der det heter at visse dokumenter, innbefattet SIRENE-håndboken, "bør" eller "skal" (på fransk "doivent") forbli fortrolige "Uavhengig av de ulike nasjonale regler". Dette er en oppsiktsvekkende intern og bindende beslutning, etter ordlyden overordnet nasjonalt regelverk.

[13] I Norge kan det tilsvarende gis forskrift om at den nylig vedtatte personopplysningsloven eller deler av den ikke skal gjelde for bestemte institusjoner og områder (personopplysningslovens § 3 tredje ledd). En tar helt klart sikte på politiets arbeidsregistre (jfr. Ot.prp. nr 92 (1998-99) s. 30-31), som i Norge på forhånd, gjennom midlertidig dispensasjon fra Datatilsynet, for eksempel er unntatt innsyn.

[14] Det vil bare være to unntak: Opplysninger om registrerte personer som oppnår statsborgerskap skal slettes, og opplysninger om registrerte personer som anerkjennes som flyktninger i henhold til FNs flyktningekonvensjon skal sperres i den sentrale databasen og skal bare kunne bli brukt i statistisk øyemed. I tillegg skal såkalte ulovlige innvandrere registreres - i praksis innvandrere som kommer til eller krysser EUs yttergrense uten gyldige papirer, noe som kan være meget krevende å skaffe seg nettopp for flyktninger fra såkalte "asylproduserende land". Man oppnådde enighet om saken (konvensjonstekst med en tilleggskonvensjon) på Ministerrådsmøtet for justis- og innenrikssaker i mars 1999, der man forutsatte at EU-kommisjonen ville legge fram et forslag til et fellesskapinstrument til å tre i stedet for både konvensjon og protokoll på bakgrunn av ikrafttredelsen av Amsterdamavtalen 1. mai 1999 (rådsreferat hentet fra Internett).

[15] Et lite eksempel: Våren 1999 holdt jeg en gjesteforelesning om de europeiske registrerings- og overvåkingssystemene ved Universitetet i Southamptons juridiske fakultet. Jeg vektla bl.a. Arbeidsgruppens arbeid, og hemmeligholdet rundt det. Under debatten etterpå reiste en tidligere politimann seg og uttalte seg frisk om de forskjellige registreringssystemene, som han så store personvernproblemer ved. Men om Arbeidsgruppen sa han: "Jeg har arbeidet i der. Arbeidet der kan jeg ikke uttale meg om, for det er hemmelig".

Adresse: Institutt for rettssosiologi
Postboks 6706 St. Olavs plass
N-0130 Oslo
E-post: thomas.mathiesen@jus.uio.no