

Kriminalomsorgens bruk av INFOFLYT-systemet - de registrertes personvern og rettssikkerhet



Universitetet i Oslo
Det juridiske fakultet

Kandidatnummer: 590
Leveringsfrist: 25.04.2010

Til sammen 17654 ord

Innholdsfortegnelse

<u>INNLEDNING</u>	1
1.1 Bakgrunn	1
1.2 Tema og problemstilling	3
1.3 Avgrensning	4
1.4 Begrepsavklaring	6
1.4.1 Personvern	6
1.4.2 Rettssikkerhet	7
1.4.3 Register	8
<u>2 OM INFOFLYT</u>	10
2.1 De registrerte	10
2.1.1 Innsatte	10
2.1.2 Innsattes personkrets	11
2.1.3 Risikogruppen	11
2.2 Opplysninger som omfattes	11
2.3 Kompis-systemet	12
2.4 Nasjonalt register	13
2.4.1 Antall registrerte	13
<u>3 RETTSKILDEBILDET</u>	15
3.1 Lover	16
3.2 Forarbeid	17

3.3	Andre myndigheters praksis	17
3.4	Retningslinjer	19
3.5	Internasjonale konvensjoner og praksis	19
3.6	Hensyn	22
4	<u>TILFREDSTILLER INFOFLYTT KRAVENE TIL BEHANDLING AV PERSONOPPLYSNINGER?</u>	24
4.1	Grunnleggende vilkår i personopplysningsloven §8 jf §9	24
4.1.1	Hjemmelsgrunnlaget ”samtykke”	25
4.1.2	Hjemmelsgrunnlaget ”fastsatt i lov”	25
4.1.3	Hjemmelsgrunnlaget ”nødvendig”	28
4.1.4	Tilleggsvilkår for behandling av sensitive opplysninger	29
4.2	Formålskravet etter pol. §11 bokstav b og c	31
4.3	Relevanskravet	32
4.4	Krav til opplysningskvalitet og sletting	33
4.5	Vilkår etter EMK	36
4.5.1	Lovskravet i EMK	37
4.5.2	Nødvendighetsvilkåret i EMK	40
4.6	Konsesjonsspørsmålet	42
4.7	Forholdet til ny lovgivning	42
5	<u>ADGANG TIL UTVEKSLING AV OPPLYSNINGER MELLOM KRIMINALOMSORGEN OG POLITIET</u>	44
5.1	Kriminalomsorgen	45
5.2	Politiet	46
5.2.1	Kan politiet pålegge kriminalomsorgen taushetsplikt?	47

<u>6</u>	<u>INNSYNSRETT OG INFORMASJONSPLIKT</u>	<u>49</u>
6.1	Informasjonsplikten	49
6.2	Generell og individuell innsynsrett	52
6.3	Unntak jf pol. §§19(2) og 20(2)	52
6.4	Unntak etter pol. §23	53
6.5	Unntak jf strgjfl. §7 bokstav c	55
6.6	Meroffentlighet	57
<u>7</u>	<u>KLAGE- OG KONTROLLORDNINGER</u>	<u>59</u>
7.1	Datatilsynet	59
7.2	Klage til overordnet forvaltningsorgan	60
7.3	Sivilombudsmannen	62
7.4	Retten til effektiv prøving jf EMK art 13	64
7.5	Retten til adgang til domstolene jf EMK art.6	65
<u>8</u>	<u>SLUTTKOMMENTARER</u>	<u>66</u>
<u>9</u>	<u>LITTERATURLISTE</u>	<u>69</u>
9.1	Lov	69
9.2	Forskrifter	70
9.3	Rundskriv/retningslinjer	70
9.4	Konvensjoner/direktiv	70

9.5 Forarbeider	71
9.6 Rettspraksis	72
9.7 Andre myndigheters praksis	72
9.8 Litteratur	73
9.9 Annet	74

INNLEDNING

1.1 Bakgrunn

Natt til mandag 30. august 2004. En pengetransport ranes på Aker brygge. Ranere bevæpnet med maskinpistol og håndvåpen stripser vekterne. Skudd avfyres da tre velkjente kriminelle pågripes på stedet. En av ranerne hadde permisjon fra Oslo fengsel fra soning av en dom på 6 års fengsel for kidnapping, tortur og drapstrusler.

Aker Brygge-ranet utløste stor debatt i mediene. Riksadvokaten satte i gang undersøkelser om hvorfor de tre var på frifot da ranet ble begått. På Stortinget fikk justisministeren spørsmål om oppfølgingen av reglene for permisjon under soning.

I ministerens svar omtales INFOFLYT-systemet som et eget verktøy med hensyn til sikkerhetsvurderinger av innsatte: ”Infoflyt-systemet mellom politiet og kriminalomsorgen er operativt og vil være et viktig verktøy i denne forbindelse”.¹ Ministeren viste videre til et kommende rundskriv som skulle omhandle samarbeid mellom kriminalomsorgen og politiet/påtalemyndighet.

Dette er så langt jeg har klart å bringe på det rene, første gang INFOFLYT-systemet omtales i offisielle dokumenter.

I mars 2005 utga Justis- og politidepartementet (heretter departementet) rundskriv G-3/2005 ”Informasjonsutveksling mellom kriminalomsorgen og politiet/påtalemyndigheten” (heretter G-3/2005). Hvoretter kriminalomsorgens sentrale forvaltning (KSF) utga rundskriv KSF 2/2005 ”INFOFLYT – Særskilt saksbehandlingsinstruks” (heretter KSF 2/2005).

I følge opplysninger fra tjenestemenn i politiet og kriminalomsorgen, har det ”alltid” foregått et samarbeid og informasjonsutveksling om innsatte i norske fengsler og

¹ Stortinget, dok.nr.15:877(2003-2004)

forholdene rundt dem. INFOFLYT-systemet kan dermed anses som et forsøk på formalisering av et uregulert samarbeid som har pågått over tid.

I G-3/2005 heter det at informasjonsutvekslingen ”må systematiseres og kvalitetssikres i størst mulig grad”. Politiet og kriminalomsorgen instrueres til å benytte INFOFLYT-systemet for informasjonsutveksling ”om særlig alvorlige saker og med særlig høy risiko”. KSF har i denne forbindelse opprettet et sentralt register med sensitive opplysninger om innsatte, innsattes personkrets og andre.² INFOFLYT-registeret kommer i tillegg til kriminalomsorgens sentrale datasystem, KOMPIS, som registrerer samtlige innsatte i norske fengsler.

Informasjonsutvekslingen omfatter opplysninger av varierende kvalitet; alt fra enkeltstående kildeopplysning til informasjon fremkommet gjennom et lengre etterretnings- og etterforskningsarbeid kan være INFOFLYT-registrert.

Opplysningene brukes av kriminalomsorgen til å foreta riktige ”sikkerhetsmessige vurderinger”.³ Vurderingene kan ha som formål å beskytte liv og helse til vitner, informanter eller ansatte i fengslene, og for å bekjempe og forebygge kriminalitet. For eksempel kan politiet ha opplysninger om at en innsatt planlegger å begå et væpnet ran under neste permisjon. Dette formidles til kriminalomsorgen når politiet får vite at det foreligger en permisjonssøknad. Med bakgrunn i opplysningene, avslår fengselet permisjonssøknaden. Dermed kan en alvorlig kriminell handling med fare for liv og helse, være avverget.

Innsatte som ”settes på INFOFLYT” er underlagt et særskilt inngripende overvåknings- og kontrollregime. Beslutningene som fattes med bakgrunn i INFOFLYT-opplysninger, kan være av svært inngripende karakter og ha omfattende konsekvenser for den innsattes soningsprogresjon. I tillegg til permisjonsnektelse kan INFOFLYT medføre vedtak om innsettelse på avdelinger med særlig høyt sikkerhetsnivå, overføringer til lukkede fengsler,

² KSF 2/2005 pkt.2

³ KSF 2/2005 pkt.1

innsetting på enerom (isolasjon), besøksnektelser, avslag på søknad om åpen soning og avslag på søknad om prøveløslatelse.

Det kan også fattes beslutninger som berører tredjeperson, for eksempel at enkelte personer nektes å besøke innsatte eller at kontakten de har med innsatte underlegges strengere kontroll enn det normalt ville vært uten den aktuelle INFOFLYT-registreringen.

Konsekvenser for registrerte som verken er straffedømte eller tilhører den innsattes personkrets, er vanskelig å vurdere. Det vil blant annet være avhengig av type opplysninger, hvor lenge de lagres i systemet, hvem som får tilgang til dem og hva de senere eventuelt brukes til.

1.2 Tema og problemstilling

Oppgavens hovedproblemstilling er i hvilken grad kriminalomsorgens bruk av INFOFLYT-systemet tilfredstiller kravene til behandling av sensitive personopplysninger. Jeg vil foreta en vurdering av om dagens regelverk i tilstrekkelig grad ivaretar hensynene til rettssikkerhet og personvern.

Regelverket for denne spesielle og inngripende behandling av personopplysninger er så vagt og uklart at arbeidet med å få oversikt over selve rettskildebildet ble svært omfattende i seg selv.

Selv om formålet med INFOFLYT er legitimt, er det viktig at det er etablert klare regler og kontrollordninger som ivaretar rettssikkerheten for de registrerte. Spesielt viktig er dette når personer som verken er innsatte, tilhører den innsattes personkrets eller har begått kriminalitet, også omfattes av INFOFLYT. Grunnlaget for at kriminalomsorgen som har straffegjennomføring som hovedoppgave, lovlig kan registrere og behandle opplysninger om personer som ikke har direkte tilknytning til kriminalomsorgen, er spesielt vanskelig å se noe.

Et uklart regelverk vil kunne åpne for misbruk. Selv om det rent faktisk ikke begås misbruk, vil manglende eller uklare regler allikevel kunne gå ut over den tillitt og notoritet et slikt system bør ha. Etter legalitetsprinsippet er kravet til klar lovhjemmel sterkere jo mer

inngrepene er. Hjemmelsgrunnlaget for INFOFLYT vurderes i kapittel 4 og klage- og kontrollordningene i kapittel 7.

I tillegg til at regelverket er uklart, gis det som utgangspunkt ikke innsyn i opplysningene i INFOFLYT verken til den registrerte eller dennes advokat.⁴ Det betyr at avgjørelser av inngrepene fattes etter en skjønnsmessig vurdering av sensitive personopplysninger, uten at den det gjelder får vite grunnlaget for avgjørelsen. Dette gir den registrerte liten mulighet til å angripe avgjørelsen. Hvorvidt en slik regelforståelse er i samsvar med gjeldende rett, behandles i kapittel 6.

Gjennom blant annet menneskerettslige og EØS-rettslige forpliktelser er det utledet flere grunnleggende personvern- og rettssikkerhetsprinsipper som Norge er forpliktet til å ivareta. Retten til et privatliv er nedfelt i den Europeiske menneskerettskonvensjonen (heretter EMK) art.8.

For mange er det kanskje ikke innlysende at en som sitter i fengsel har rett til et personvern fordi en fange ikke har et tradisjonelt privatliv. Fengselsstraff innebærer jo nettopp kontinuerlig kontroll av varierende grad. Etter Den Europeiske menneskerettighetsdomstols (EMD) praksis skal imidlertid sentrale rettigheter ikke settes til side i større grad enn nødvendig for å gjennomføre soningen. Fanger har også rett til personvern og respekt for den eventuelle rest som er igjen av et privatliv i fengselet. Inngrep i privatlivet tillates bare dersom det hjemles i lov, er nødvendig i et demokratisk samfunn og ivaretar relevante formål, jf EMK art.8(2). Hvorvidt INFOFLYT oppfyller disse vilkårene vurderes i pkt. 4.5.

1.3 Avgrensning

Av plasshensyn er oppgaven begrenset til *kriminalomsorgens* bruk av INFOFLYT. Vurderinger av politiets bruk av systemet berøres bare noen steder der det har betydning for kriminalomsorgens håndtering av opplysninger.

⁴ KSF 2/2005 pkt.8

INFOFLYT omfatter både varetektsinnsatte som ennå ikke har fått pådømt saken, og soningsinnsatte som har fått sin sak rettskraftig avgjort.

Varetektsinnsatte behandles etter reglene som gjelder *innenfor* straffesaker. Grunnlaget for inngrep mot dem vil i stor grad være gjenstand for jevnlig og fornyet rettslig prøving under hele varetektsoppholdet jf straffeprosesslovens regler.

Gjennomføring av rettskraftig fengselsstraff, ligger under kriminalomsorgens myndighet jf straffegjennomføringsloven (strgjfl.) §5. Når det gjelder soningsdømte, følger derfor behandling av opplysninger i INFOFLYT reglene som gjelder *utenfor* straffesaker. I motsetning til varetektsinnsatte, er det ikke retten men kriminalomsorgen som gjennom enkeltvedtak etter forvaltningslovens regler, fatter avgjørelser om inngrep mot de soningsinnsatte. Den manglende muligheten for raskt og jevnlig å kunne bringe avgjørelsen inn for domstolen, er en sentral forskjell mellom de to fangegruppene.

Av hensyn til oppgavens omfang og at varetektsinnsatte har helt andre klage- og kontrollmuligheter som følge av reglene i straffeprosessloven, vil oppgaven begrense seg til å omhandle de soningsinnsatte, deres personkrets og ”risikogruppen”⁵.

Noen ganger kan soningsinnsatte være siktet i andre saker mens de soner og er dermed å betrakte også som varetektsfanger. Slike spesialtilfeller behandles heller ikke.

INFOFLYT omfatter i tillegg til samarbeid med det ordinære politiet også informasjonsutveksling mellom kriminalomsorgen og politiets sikkerhetstjeneste (PST). Dette vil typisk være i saker hvor PST har vært det førende organet under etterforskningen og iretteførselen, men kan også være i andre saker. I PST-saker vil vurderinger som ”av hensyn til rikets sikkerhet” ha betydning for behandling av opplysninger, innsynsretten mv. Av hensyn til oppgavens omfang vurderes ikke disse spesielle hensynene. Utgangspunktet er imidlertid at også i PST-saker skal kravene til saksbehandling og hjemmelsgrunnlag, være de samme som i ”ordinære” politisaker.

Som part i forvaltningssak, har den registrerte mulighet til å gå til sivil sak for å få prøvet vedtaket og derigjennom få innsyn i kriminalomsorgens beslutningsgrunnlag. Prosessen vil

⁵ Se pkt.2.1.3

imidlertid ta tid. Muligheten er derfor stor for at den registrerte før det foreligger en avgjørelse, vil ha mistet sin rettslige interesse for å få saken prøvet og derfor som utgangspunkt ikke får behandlet saken i domstolen.⁶ Dette illustreres også ved at KSF i saksbehandlingsinstruksen for INFOFLYT, fremhever at rettskjennelser som gir parten innsyn, kan påkjæres i flere instanser og skriver videre: ”Det kan antas at slik prøving kan ta noe tid.”⁷

Muligheten for domstolsbehandling er mer teoretisk enn den er reell. På bakgrunn av dette kommer jeg ikke til å drøfte innsynsretten gjennom domstolsbehandling nærmere.

Et annet problem i forbindelse med INFOFLYT, er internkontroll. Ansvar for å etablere planlagte og systematiske tiltak for å sikre at personopplysningslovens bestemmelser følges, ligger hos den behandlingsansvarlige.⁸ KSFs rundskriv gir ingen nærmere retningslinjer for behandling av personopplysninger knyttet til dokumenter som utformes på lokalt eller regionalt nivå. Dette kan være i strid med kravene til internkontroll jf personopplysningsloven (pol.) §13. Jeg kommer av hensyn til oppgavens omfang ikke til å berøre dette nærmere.

1.4 Begrepsavklaring

1.4.1 Personvern

Det er ingen legaldefinisjon av personvernbegrepet i norsk lovgivning. Flere bestemmelser tar imidlertid sikte på å beskytte personvernet, retten til privatliv og vern om personopplysninger.

Personvernkommisjonen definerer personvern som ”ivaretagelsen av personlig integritet; ivaretagelsen av enkeltindividers mulighet til privatliv, selvbestemmelse (autonomi) og selvutfoldelse”.⁹ Kommisjonen skiller ut ”personopplysningsvernet” som en egen kategori

⁶ Jf kravet om rettslig interesse, tvisteloven §1-3(2)

⁷ KSF 2/2005 pkt.9

⁸ Pol. §14 og personopplysningsforskriften §3-1

⁹ NOU 2009:1 s.32

og definerer dette som ”regler for standarder for behandling av personopplysninger som har ivaretagelse av personvern som hovedmål”.

Kommisjonen legger til grunn at formålet med slike regler er å sikre enkeltindivider oversikt og kontroll over behandlingen av opplysninger om dem selv, og at enkeltpersoner med visse unntak skal ha mulighet til å bestemme hva andre skal få vite om hans eller hennes personlige forhold. Personvernkommisjonens forståelse legges til grunn i denne avhandlingen.

Begrepet personopplysning er definert i pol. §2 nr.1 som : ”Opplysninger og vurderinger som kan knyttes til enkeltperson.” Definisjonen kan deles opp i fire elementer: 1) enhver form for informasjon som 2) kan knyttes til 3) en identifisert eller identifiserbar 4) fysisk person.¹⁰ Vurderingen av om en opplysningstype faller inn under lovens definisjon av personopplysninger er avgjørende for om personopplysningsloven kommer til anvendelse.

1.4.2 Rettssikkerhet

Personvern og rettssikkerhet nevnes ofte i sammenheng. Ivaretagelsen av personvernet er ofte ansett å innebære ivaretagelsen av rettssikkerheten og omvendt.¹¹

Kjernen i begrepet ”rettssikkerhet” er knyttet til sikkerhet mot overgrep og vilkårlighet fra staten samtidig som vedkommende skal ha mulighet til å forutberegne sin rettsstilling og ivareta sine rettslige interesser.

Mens personvernreglene skal verne enkeltmenneskets private sfære og personlige forhold mot uønsket inngrep fra staten og andre borgere, tar rettssikkerhetsbegrepet sikte på å beskytte mot vilkårlig inngrep fra statsmakten og sikre den enkeltes rettigheter i forhold til det offentlige.¹²

Rettssikkerhet er et hensyn som står sentralt innenfor forvaltningsrettens, strafferettens og straffeprosessens område. Materiell rettssikkerhet stiller overordnede krav til avgjørelsens innhold. Legalitetsprinsippet er helt sentralt; inngrepene må ha hjemmel i lov. Hjemmelen

¹⁰ Ibid. pkt.4.5.3

¹¹ Ibid. pkt.4.1.6.

¹² Bernt/Rasmussen, s.42

danner rammen for et rettmessig inngrep og dermed også for hva som er å betrakte som overgrep og vilkårlighet. Hensynet til forutberegnelighet står også sentralt. Det innebærer at hjemmelen for inngrep skal være tilstrekkelig klar og presis slik at den enkelte kan forutberegne sin rettsstilling og dermed innrette seg etter og forsvare seg mot inngrepet. Det er videre et krav om forholdmessighet mellom kriminaliteten som bekjempes og inngrepet som gjøres i den enkeltes personvern.

Prosessuell rettssikkerhet angir kravene til hvordan avgjørelsen blir truffet og omfatter kravene til saksbehandling for iverksetting og kontroll av de aktuelle inngrepene, herunder spørsmål om kontradiksjon, innsyn og underretning. Også krav til avgjørelsens utforming og overprøving er elementer under den prosessuelle rettssikkerheten.

1.4.3 Register

Tradisjonelt har man med ”registrering” ment en nedtegning av personopplysninger i form av systematisk lagring, slik at opplysninger om den enkelte kan finnes igjen. Den tradisjonelle definisjonen av ”registrering” er lite hensiktsmessig i forhold til elektronisk behandling der alle opplysninger kan gjenfinnes uavhengig av om de er lagret systematisk eller ikke.

Politiregisterutvalget påpekte at den tradisjonelle definisjonen vil kunne skape uklarhet om hvilke regler som gjelder for opplysninger som ennå ikke er plassert i noe register. Utvalget mente at selve registreringen bare vil være en form for, eller del av behandling av opplysninger der senere systematisering, oppbevaring, retting, utveksling, innsyn, sperring og sletting er eksempler på andre deler.¹³

Den nye politiregisterloven angir at loven kommer til anvendelse for elektronisk behandling av opplysninger uavhengig av om opplysningene inngår i et register. I tillegg kommer loven til anvendelse for manuell behandling av opplysninger når de inngår eller skal inngå i et register.¹⁴ Politiregisterloven definerer register som ”en samling opplysninger

¹³ NOU 2003:21

¹⁴ Politiregisterloven §3(3)

som er lagret systematisk på en slik måte at opplysninger om den enkelte kan finnes igjen”.¹⁵

Behandling av opplysninger blir definert som ”enhver elektronisk eller manuell bruk av opplysninger, som for eksempel innsamling, registrering, systematisering, oppbevaring, tilpasning, endring, gjenfinning, søking, videreformidling ved overføring, spredning eller andre former for tilgjengeliggjøring, sammenstilling eller samkjøring, sperring, sletting eller tilintetgjøring eller en kombinasjon av slike bruksmåter”.¹⁶

Personopplysningsloven bygger også på et slikt utvidet behandlingsbegrep og at begrepet således er tvetydig i form av at ”behandling” er en samling opplysning i form av et register eller et system.

Personopplysningsloven definerer personregistre som ”registre, fortegnelser mv der personopplysninger er lagret systematisk slik at opplysninger om den enkelte kan finnes igjen”, jf pol. §2 nr.3.

”Behandling av personopplysninger” defineres som: ”enhver bruk av personopplysninger, som feks innsamling, registrering, sammenstilling, lagring og utlevering eller en kombinasjon av slike bruksmåter”, jf pol.§2 nr.2.

Jeg legger det utvidede behandlingsbegrepet til grunn i denne avhandlingen.

¹⁵ Politiregisterloven §2 nr.3

¹⁶ Politiregisterloven §2 nr.2

2 Om INFOFLYT

2.1 De registrerte

De INFOFLYT-registrerte kan grovt inndeles i tre grupper: *innsatte*, *innsattes personkrets* og det jeg her vil kalle ”*risikogruppen*”.¹⁷

2.1.1 Innsatte

Den første gruppen er *innsatte* som antas å medføre en særlig rømningsfare, fare for anslag utenfra for å bistå til rømning eller gisseltaking, fare for ny særlig alvorlig kriminalitet og innsatte med spesielle beskyttelsesbehov (for eksempel i forbindelse med vitnebeskyttelse). Tilknytning til organiserte kriminelle nettverk, terrorister, politiske eller religiøse ekstreme nettverk er i instruksene beskrevet som kumulativt vilkår for å bli registrert i INFOFLYT. I tillegg kan det tas hensyn til lovbruddets art, lengden på dommen og tidligere atferd i fengsel.

Målgruppen omfatter også innsatte tilknyttet særskilte kriminelle nettverk hvor den enkelte ikke nødvendigvis anses å utgjøre en særlig risiko, men hvor to eller flere tilknyttet samme nettverk i samme fengsel, kan anses å utgjøre en risiko. Som eksempler på slike nettverk nevner instruksene ”ransmiljøer”, ”mc-kriminelle”, ”visse torpedo/voldsmiljøer”, ”særskilte narkotikaligaer”, ”satanister” og ”aktive gjengmedlemmer”.¹⁸

¹⁷ KSF 2/2005 pkt.3

¹⁸ KSF 2/2005 pkt.3

2.1.2 Innsattes personkrets

Den andre gruppen som omfattes av INFOFLYT, er personkretsen som er knyttet til de nevnte grupper innsatte. Som eksempel på denne personkretsen nevnes besøkende, telefonkontakter, mottakere/avsendere av korrespondanse og annen kommunikasjon til og fra de innsatte.¹⁹

2.1.3 Risikogruppen

Den tredje gruppen som omfattes av INFOFLYT-registrering, er en personkrets som *ikke* er innsatte, men som "antas å ha tilhørighet" til organiserte kriminelle nettverk, terrorister, politiske ekstreme nettverk eller religiøse ekstreme nettverk, "og som vil kommunisere eller kommuniserer med innsatte"... "også selv om de innsatte i utgangspunktet ikke omfattes av målgruppen".²⁰ Denne personkretsen vil jeg omtale som "risikogruppen".

2.2 Opplysninger som omfattes

Bortsett fra de nevnte tilknytninger til diverse nettverk samt vurderinger av risikofaren ved den enkelte, spesifiserer instruksene ikke hva slags type informasjon som registreres utover i generelle vendinger.

Det oppgis at opplysninger kriminalomsorgen trenger for å "beslutte riktige sikkerhetsmessige tiltak" skal behandles i INFOFLYT-systemet. Som eksempel nevnes opplysninger om de omtalte målgruppene som er "fremkommet under politiets etterforskning eller etterretning". Videre behandles og utveksles informasjon som politiet trenger for å forebygge og bekjempe kriminalitet knyttet til samme målgruppe.²¹

Dessuten registreres og behandles også mye av samme type informasjon som i Kompis når det gjelder opplysninger som gis fra kriminalomsorgen til politiet.

Det betyr at opplysninger både *i* og *utenfor* straffesaker behandles i systemet.

¹⁹ l.c.

²⁰ l.c.

²¹ KSF 2/2005 pkt.4

2.3 Kompis-systemet

Innsatte som er på INFOFLYTT vil være særskilt markert i Kompis-KIA, som er et av tre sentrale datasystemer i kriminalomsorgen hvor alle innsatte er registrert.²²

Registreringene i INFOFLYTT vil ikke komme opp i Kompis annet enn som en merking på den innsattes personbilde. Dette skal gjøre brukeren oppmerksom på at overordnet må kontaktes før ny beslutning tas om vedkommende.²³

I Kompis behandles følgende opplysninger om alle innsatte i norske fengsler:

Navn, alias/tidligere navn, fødselsnummer, kjønn, folkeregistrert adresse, utenlandsadresse, fødested, statsborgerskap, innsattnummer, innsattkategori (varetekt, sikring, forvaring, bøtesoning mv.), yrkesstatus, sivilstatus, bidragsplikt, språk, plassering i anstalten, status for soning (lukket avdeling, åpen avdeling, behandling sinstitusjon, sykehus), utdrag fra dom.²⁴

Videre registreres opplysninger om ”hendelser”, for eksempel at det er skrevet miljørapport, behandlet permisjonssøknader, gitt disiplinærreaksjon, tatt blod- eller urinprøver med resultater, at vedkommende har hatt besøk osv. Opplysninger om pårørende og navn på besøkende registreres. Dessuten er det et fritekstområde for hver enkelt innsatt.

Behandlingen av personopplysninger i Kompis anses som svært inngripende da registreringene er klart sensitive i personopplysningslovens forstand.²⁵ Registreringen i Kompis, er vurdert å innebære en svært omfattende kartlegging av den enkelte innsattes liv.²⁶ Når registreringene i Kompis ikke vurderes å være omfattende nok til at kriminalomsorgen mener de kan foreta forsvarlige sikkerhetsvurderinger av visse grupper innsatte og andre, kan man uten videre slutte at INFOFLYTT innebærer ytterligere kartlegging. INFOFLYTT må derfor anses å være mer inngripende enn behandlingen tilknyttet Kompis.

²² Kriminalomsorgen.no

²³ KSF 2/2005 pkt.6

²⁴ Datatilsynet, kontrollrapport 07/01455

²⁵ Pol. §2 nr.8

²⁶ Datatilsynet, kontrollrapport 07/01455

2.4 Nasjonalt register

INFOFLYT omtales som eget register i flere av punktene i KSF 2/2005. I rundskrivets punkt 6 heter det ”I KSF vil opplysningene lagres og bearbeides i eget register, INFOFLYT-registeret”.

Videre skal INFOFLYT-mappene som opprettes i fengslene, holdes atskilt fra øvrige fangesaker og sikres i eget låst skap. Utover en markering på den innsattes personbilde i Kompis, er INFOFLYT-registeret verken elektronisk eller fysisk en del av KOMPIS. Kvantitativt og kvalitativt sett behandles flere sensitive opplysninger enn registreringene i KOMPIS. En vesentlig forskjell er dessuten at INFOFLYT også åpner for registreringer av informasjon om personer som verken er innsatte, dømte, pårørende eller besøkende. Etter personopplysningslovens definisjon av ”register”, er det etter dette vanskelig å forstå rundskrivet på annen måte enn at KSF har etablert et eget nasjonalt INFOFLYT-register som ikke kan anses å være en del av Kompis.

2.4.1 Antall registrerte

FNs arbeidsgruppe for vilkårlig frihetsberøvelse fikk under sitt besøk i Norge i 2007 opplyst at ca 50 innsatte over hele landet var registrert i INFOFLYT og at tallet var stigende.²⁷

I brev til Sivilombudsmannen i 2009²⁸, opplyste departementet at det inntil da var behandlet ca 150 personer i systemet og at det pr brevets dato var ca 35 personer registrert. Med tanke på at det i gjennomsnitt i 2007 og 2008 befant seg henholdsvis 3295²⁹ og 3420³⁰ innsatte i norske fengsler, er det en marginalisert gruppe personer som behandles i INFOFLYT-systemet.

Selv om det foreligger muligheter for misbruk blant annet pga uklar regulering og mangelfull ekstern kontroll av systemet,³¹ tyder det forholdsvis lave antall registrerte på at INFOFLYT-systemet kvantitativt sett ikke misbrukes. Dette forutsetter imidlertid at det

²⁷ FN, A/HRC/7/4/ADD.2

²⁸ Justis- og politidepartementet, 21.09.2009

²⁹ Kriminalomsorgens årsmelding 2007

³⁰ SSB

³¹ Se kap.4 og 7

oppgitt antall registrerte rent faktisk er korrekt. Etter pol. §2 nr.6 er definisjonen på en registrert ”den som en personopplysning kan knyttes til”. Det betyr at også ”den innsattes personkrets” og personer i ”risikogruppen” skal regnes som ”registrert”. Det har imidlertid ikke vært mulig å få avklart om det oppgitte totalantallet på ”ca. 150 personer” inkluderer *samlige* registrerte eller om det bare inkluderer antallet *innsatte* som er/har vært på INFOFLYT.³²

At systemet kvantitativt sett ikke anses misbrukt, utelukker for øvrig ikke at det kan foregå uforholdsmessige inngrep overfor den enkelte.

³² KSF ikke har besvart gjentatte henvendelser vedrørende dette under arbeidet med avhandlingen

3 Rettskildebildet

I utgangspunktet legges alminnelig rettsdogmatisk metode til grunn. Det metodisk særskilte i vurderingen av INFOFLYT, er imidlertid at rettskildebildet preges av at det knapt eksisterer rettskilder av høyere trinnhøyde som direkte omhandler INFOFLYT. Fordi rettskildebildet er uklart og vagt, er det viet relativt stor plass til å gjøre rede for hvilke rettskilder som kan ha betydning for vurderingene tilknyttet INFOFLYT.

Det er ingen særskilt lovhjemmel for INFOFLYT. Retningslinjer i form av rundskriv og instruksjoner som i et rikere rettskildebilde ville hatt mindre vekt, vil her danne utgangspunktet for vurderingen av systemet.³³ Flere av retningslinjene er graderte og ikke tilgjengelige verken for offentligheten eller de registrerte. Hemmeligholdet bidrar til å skape inntrykk av et uklart rettsbilde.

Ingen saker om INFOFLYT er hittil prøvet for Høyesterett. Det har ikke vært mulig å finne noen underrettsavgjørelser. Kriminalomsorgens avgjørelser om forhold vedrørende innsatte er enkeltvedtak som ikke er allment kjent på grunn av taushetsplikten.³⁴ Forvaltningspraksis er derfor ikke mulig å benytte som rettskilde i denne oppgaven. I et slikt rettskildebilde, vil Sivilombudsmannens praksis få større vekt enn om rettskildene hadde vært flere og av høyere trinnhøyde.³⁵ Det samme vil gjelde Datatilsynets uttalelser som ekspertorgan på området for behandling av personopplysninger.

³³ Se pkt.3.4

³⁴ Fvl. §13

³⁵ Se pkt.3.3

Norge har gjennom ulike internasjonale forpliktelser, bundet seg til å overholde en rekke konvensjoner. Særlig på personvern- og rettssikkerhetsområdet danner internasjonalt regelverk ramme for utformingen og praktiseringen av nasjonal rett.³⁶

3.1 Lover

INFOFLYT for soninginnsette hører inn under fengselsretten som er en spesiell del av forvaltningsrett. Det er dermed to sett av regler å forholde seg til. Rettskildene er i prinsippet de samme som ellers i forvaltningen.

Fengselsrett reguleres av straffegjennomføringsloven med tilhørende forskrifter.

Forvaltningslovens saksbehandlingsregler gjelder for kriminalomsorgen jf strgjfl. §7.

Personopplysningsloven gir generelle bestemmelser om behandling av personopplysninger.

Loven gjelder i utgangspunktet for all elektronisk og manuell behandling av personopplysninger i offentlig så vel som privat sektor jf pol.§3 bokstav a. Det følger av pol. §5 at bestemmelsene kommer til anvendelse ”om ikke annet følger av særskilt lov som regulerer behandlingsmåten”.

Som spesiallov går straffegjennomføringsloven foran personopplysningsloven, men i de tilfeller der straffegjennomføringsloven er taus eller ikke gir tilstrekkelig klar hjemmel for den behandling av personopplysninger som finner sted, vil personopplysningsloven komme til anvendelse.

Etter gjeldende rett er strafferegisterloven den sentrale hjemmelen for politiets behandling av personopplysninger. Strafferegistreringsloven med tilhørende forskrifter sier imidlertid lite om hvordan personopplysninger skal behandles. Politiregisterutvalget legger til grunn at personopplysningsloven kommer til anvendelse der strafferegistreringsloven er taus.³⁷

Behandling av opplysninger i tilknytning til straffesaker reguleres av straffeprosessloven og faller utenfor personopplysningslovens virkeområde.³⁸ Personopplysningslovens

³⁶ Se pkt.3.5

³⁷ NOU 2003:21, s.104

³⁸ Personopplysningsforskriften §1-3

bestemmelser vil etter dette regulere politiets behandling av personopplysninger *utenfor* straffesaker.

I forarbeidene til personopplysningsloven fremholdes det at regelverket for politiets personregistre er uoversiktlige og at strafferegistreringsloven inneholder få materielle regler.³⁹ Den nye politiregisterloven som Stortinget vedtok i mars 2010, forventes å bøte på noen av manglende ved dagens regelverk. Departementet opplyser at ”ikrafttredelse av loven forventes å bli høsten 2011”.⁴⁰

3.2 Forarbeid

INFOFLYT-systemet er lite direkte omtalt i ordinære forarbeider som odelstingsproposisjoner, Norges offentlige utredninger og proposisjon til Stortinget. Det er imidlertid relativt rikt omfang av forarbeider når det gjelder tema som personvern, rettssikkerhet, taushetsplikt og kriminalitetsbekjempelse. Disse temaene henger ofte sammen og innvirker på hverandre, og de er derfor gjerne omtalt i de samme forarbeidene.⁴¹

3.3 Andre myndigheters praksis

Datatilsynet har på bakgrunn av en rekke klager fra innsatte, gjennomført kontroll av behandlingen av personopplysninger om innsatte ved norske fengsler.⁴² Selv om kontrollen særlig gjaldt behandling i Kompis, vil mange av funnene være gjeldende også for behandling av personopplysninger i INFOFLYT.

³⁹ Ot.prp.nr 92(1998-1999) pkt.6.4

⁴⁰ Departementet, e-post, april 2010

⁴¹ F.eks. NOU 1997:19, NOU 2003:21, NOU 2009:1, NOU 2009:15, St.meld.nr.37(2007-2008), Ot.prp.nr.5(2000-2001), Ot.prp.nr.108(2008-2009)

⁴² Datatilsynet, kontrollrapport 07/01455

FNs arbeidsgruppe for vilkårlig frihetsberøvelse uttrykker i sin rapport av oktober 2007, bekymring for manglende rettssikkerhet for de registrerte. Arbeidsgruppen ser på INFOFLYT-systemet som et ”issue of concern”.⁴³

Sivilombudsmannen har behandlet noen få klagesaker fra innsatte i forbindelse med INFOFLYT.⁴⁴ Eventuelle årsaker til det lave antall klagesaker kommer jeg tilbake til i kapittel 7.

På bakgrunn av klagesakene, Datatilsynets kontroll og rapporten fra FNs arbeidsgruppe, har Sivilombudsmannen tatt opp sak ”av eget tiltak”.⁴⁵ I anledning saken har ombudsmannen bedt departementet besvare spørsmål om det rettslige grunnlaget for KSFs rundskriv 2/2005 og rettslig grunnlag for behandling av personopplysninger samt spørsmål vedrørende opplysningsplikt, innsynsrett, retting og sletting av opplysninger. Saken er ikke ferdigbehandlet.

Sivilombudsmannen er oppnevnt av Stortinget for å hindre at den enkelte utsettes for urett i forvaltningen og for å bidra til at offentlig forvaltning respekterer og sikrer menneskerettighetene.⁴⁶ Selv om ombudsmannen ikke kan treffe bindende vedtak i en sak og er begrenset i sin adgang til å kritisere skjønnsutøvelsen, hører det med til sjeldenhetene at forvaltningsorganene ikke retter seg etter ombudsmannens uttalelser. Ordningen med ombudsmann bygger på at uttalelsene har en slik autoritet at forvaltningen normalt vil bøye seg for dem.⁴⁷

Ombudsmannens rolle er spesielt viktig på et område som fengselsrett som i så sterk grad preges av at persongruppen som berøres, befinner seg i en tvangssituasjon og at mange av dem er personer med begrensede ressurser.

⁴³ FN, A/HRC/7/4ADD.2

⁴⁴ Ombudsmannssak 2006/1502 og 2007/264

⁴⁵ Ombudsmannssak 2007/2274

⁴⁶ Sivilombudsmannsloven §3

⁴⁷ Andenæs, s.124-125

3.4 Retningslinjer

Rundskriv er direktiver og retningslinjer gitt fra overordnet til underordnet forvaltningsorgan blant annet angående hvordan lovbestemmelser skal forstås og hvilke hensyn som skal vektlegges ved skjønsmessige avgjørelser. Som rettskilde kan rundskriv bidra til å presisere en lovtekst som er meget skjønsmessig vurdert og hvor det mangler tunge rettskildefaktorer som kan trekke opp grensen.

I rundskrivsform, G-3/2005, har departementet gitt en orientering om tolkninger av lover og forskrifter i forbindelse med INFOFLYT. Med hjemmel i departementets rundskriv, har KSF gitt retningslinjer i KSF 2/2005. POD og PST opplyser at organene jf G-3/2005 har utarbeidet hver sine instruks vedrørende INFOFLYT, men at instruksene er klausulerte etter den gamle offentlighetsloven §6a og i sin helhet unndratt offentligheten.

I forbindelse med arbeidet med avhandlingen, fortalte polititjenestemenn meg at årsaken til klausuleringen var at instruksene inneholdt beskrivelse av målgruppene for INFOFLYT og at politiet ønsket å hemmeligholde dette. Med henvisning til at KSF omtaler målgruppene i sin ugraderte instruks, begjærte jeg innsyn både hos PST og POD.

POD innvilget innsynsbegjæringen med følgende begrunnelse: ”Idet kriminalomsorgens rundskriv er offentliggjort finner vi å kunne gi innsyn i direktoratets rundskriv⁴⁸ i forbindelse med ditt forskningsarbeid”. Instruksene er ikke avgradert og er dermed fortsatt ikke offentlig tilgjengelig verken for allmennheten eller de registrerte.

PST har ikke besvart innsynsbegjæringen.

3.5 Internasjonale konvensjoner og praksis

Av særlig betydning i denne sammenheng, er FN-konvensjonen om sivile og politiske rettigheter av 1966 (SP), EMK og praksis fra EMD, personverndirektivet⁴⁹ og rammebeslutningen om personvern i tredje søyle⁵⁰.

⁴⁸ POD 2005/00319

⁴⁹ EF-direktiv 95/46, inntatt i EØS-avtalen og dermed folkerettslig bindende for Norge

⁵⁰ Europarådets rammebeslutning 2008/977/JIS om vern av personopplysninger ved behandling av opplysninger i forbindelse med politisamarbeid og rettslig samarbeid i straffesaker, Schengen-relevant og dermed bindende for Norge

Av særskilt betydning er EMK og SP, som gjelder som lov i Norge og ved motstrid går foran bestemmelser i annen lovgivning jf menneskerettsloven (mrl.) §2 jf §3. Menneskerettsloven har ikke grunnlovsrang, men går foran vanlig nasjonal lov gjennom forrangsprinsippet. EMK gjelder altså direkte som norsk lov. Dette har betydning i forhold til INFOFLYT fordi norske myndigheter dermed ikke fritt kan bestemme for eksempel hva som anses som ”inngrep”, men må forholde seg til hva som er ”inngrep” etter EMK art.8. De særlige internasjonale tolkningsprinsipper som gjelder for tolkning av traktater, vil således erstatte de norske prinsipper om tolkning.⁵¹ EMD er derfor blitt en viktig prejudikatdomstol på området for internasjonale menneskerettigheter. I RT.2000 s.996 uttaler førstevoterende at norske domstoler skal benytte de samme tolkningsprinsipper som EMD og at det er tilstrekkelig å konstatere motstrid for at norsk rett må vike. Avgjørelsen er fulgt opp av senere avgjørelser. I RT.2005 s.833 finner Høyesterett at strl. §195(3) må vike for EMK art.6 nr.2 selv om det lå en klar lovvilje bak det objektive skyldkravet i forhold til alder ved seksuell omgang med barn under 14 år i norsk rett. I dommen uttales det at norske domstoler må forholde seg til konvensjonsteksten, alminnelige formålsbetraktninger og EMDs avgjørelser, men at det allikevel er EMD som skal utvikle konvensjonen. Dette kan medføre at Høyesterett fraviker sitt eget prejudikat på grunn av senere avgjørelser i EMD, noe som skjedde for eksempel i RT.2006 s.1409. Dette illustrerer at konvensjonspliktene både gjennom konvensjonstekstene og gjennom EMDs praksis, veier tungt ved tolkning og bruken av norsk rett. Retten til respekt for privatlivet er vernet bl.a. i EMK art.8 og SP art.17. EMK gir sterkere vern enn SP, og hovedregelen i EMK art.8(1) er at alle borgere har rett til ”respekt for sitt privatliv og familieliv, sitt hjem og sin korrespondanse”.⁵²

Politiregisterutvalget legger til grunn at politiets behandling av personopplysninger alltid må anses som inngripende og at opplysningene som behandles må anses som sensitive.⁵³

⁵¹ Andenæs, s.60

⁵² Se pkt.4.5

⁵³ NOU 2003:21 s.107

Praksis fra EMD har fastslått at lagring av persondata i seg selv utgjør et inngrep. Det ble blant annet fastslått i Rotaru-saken hvor retten kom til at lagring av data isolert sett, utgjorde et inngrep.⁵⁴ Lagring av persondata er på mange måter kjernen av INFOFLYT-systemet.

EMD har gradvis erkjent at EMK art.8 inneholder et personopplysningsvern. EMD har definert privatliv ("private life") relativt bredt. Domstolen fastslår at begrepet omfatter visse aktiviteter som utføres i den offentlige sfære jf blant annet Niemietz-saken.⁵⁵

Registrering og videre behandling av personopplysninger uten at den registrerte har gitt sitt samtykke til eller har fått kunnskap om behandlingen, vil i seg selv være et inngrep etter art.8(1) jf for eksempel Leander-saken⁵⁶. Når det gjelder de registrerte i INFOFLYT har de ikke samtykket til behandlingen av personopplysninger i systemet. Det synes også som om KSF og politiet ønsker at systemet skal være minst mulig kjent. Etter EMDs praksis kan en slik behandling altså bli ansett som et "inngrep".

EMK art.8 og EMDs praksis betoner videre krav til klar lovhjemmel, forutsigbarhet og proporsjonalitet/forholdsmessighet ved behandling av personopplysninger.

Ikke bare har Norge en forpliktelse til å respektere rettighetene som følger av EMK. Staten har også en plikt til å sikre rettighetene, jf. EMK art.1. Det betyr å ta positive skritt for å gjøre rettighetene effektive, blant annet å sørge for effektive kontroll- og klagemuligheter.⁵⁷

Personvernet og personopplysningsvernet står sterkt også i EU-retten. Selv om EUs personverndirektiv i utgangspunktet ikke gjelder for politisektoren jf. art.2(2), befester direktivet viktige personvernprinsipper. Det nyter dertil bred anerkjennelse og er således et av de viktigste personverninstrumentene i Europa. Sett i dette perspektivet må personverndirektivet kunne brukes som relevant tolkningsfaktor. Direktivet anses gjennomført i nasjonal rett gjennom personopplysningsloven.

⁵⁴ Rotaru mot Romania, avsnitt 46

⁵⁵ Niemietz mot Tyskland

⁵⁶ Leander mot Sverige

⁵⁷ Se kap.7 og 8

Norge har for øvrig ratifisert Europarådets personvernkonvensjon som gjelder både for offentlig og privat sektor. Den anses imidlertid ikke som folkerettslig bindende.

3.6 Hensyn

Det kan ikke oppstilles en generell regel om hvilken vekt de forskjellige hensyn skal tillegges etter straffegjennomføringsloven. I mange tilfeller vil det være flere hensyn som gjerne taler mot hverandre.

I forhold til INFOFLYT vil det typisk være en avveining mellom kriminalitetsbekjempelse og sikkerhetsmessige hensyn på den ene siden, og hensynene til rettsikkerheten og personvernet til den registrerte på den andre siden.

Generelle forvaltningsrettslige hensyn gjelder også på fengselsrettens området. Det betyr at saksbehandlingen skal foregå på en betryggende måte som sikrer riktige avgjørelser.

Likhetsprinsippet skal sikre at like tilfeller behandles likt. Det stilles krav til forutberegnelighet slik at den enkelte kan forutberegne sin rettsstilling. Effektivitet er et annet hensyn; en dom har ingen virkning dersom den ikke kan effektueres. Videre er kriminalitetens alvorlighetsgrad eller sakens karakter et eget hensyn.

”Alminnelig rettsoppfatning” er et hensyn man ofte hører brukt innen strafferett og fengselsrett. Kriminalomsorgen bruker dette hensynet som et moment når det for eksempel vurderes om en innsatt kan overføres fra et fengsel med høyt sikkerhetsnivå til et med lavere sikkerhetsnivå.⁵⁸ Hva som imidlertid til enhver tid er den ”alminnelige rettsoppfatning”, kan være vanskelig å fastslå. Dette hensynet bærer ofte preg av ”synsing” uten at oppfatningen kan befestes på vitenskapelig trygg grunn og kan derfor lett kollidere med andre hensyn som forutberegnelighet og likhetprinsippet. Det kan synes som om begrepet ofte brukes som et uttrykk for det som i virkeligheten er ens eget standpunkt.

⁵⁸ Straffegjennomføringslovens retningslinjer §9

Noe av det særskilte ved behandlingen av personopplysninger i INFOFLYT er at den foretas uten samtykke fra den registrerte, med små muligheter for innsyn og at opplysningene som brukes som beslutningsgrunnlag preges av å være av varierende kvalitet. Utfordringen for et system som INFOFLYT er å finne balansen mellom hensynet til kriminalitetsbekjempelse og hensynet til rettssikkerheten og personvernet. Demokratiske samfunn har behov for å kontrollere at individer ikke opptrer i strid med samfunnets interesser, men det er viktig å sikre at kontrollen og overvåkingen ikke blir uforholdsmessig høy.

4 Tilfredstiller INFOFLYT kravene til behandling av personopplysninger?

Etter personopplysningslovens definisjon av behandling av personopplysninger jf §2 nr.1 og nr.2, samt definisjonen av register jf §2 nr.3, faller KSFs bruk av INFOFLYT-systemet inn under lovens virkeområde.

Etter pol. §11(1)bokstavene a til e er det fem kumulative grunnvilkår som må være oppfylt for at en behandling av personopplysninger er lovlig. Den behandlingsansvarlige skal angi et klart og avgrenset formål for behandlingen, som skal være saklig begrunnet i virksomheten (bokstav b). Det vil si at man ikke kan lagre eller bruke personopplysninger på annen måte enn det er et saklig behov for i forhold til oppgavene virksomheten skal løse. Opplysningene kan ikke brukes til *mer* enn det opprinnelige formålet beskriver (bokstav c). Når formålet er oppfylt, skal opplysningene som hovedregel slettes (bokstav e). Det stilles videre krav til at opplysningene må være tilstrekkelige, korrekte, relevante og oppdaterte (bokstav d og e).

Det følger av pol. §11 bokstav a at det er et grunnleggende vilkår for å behandle personopplysninger, at et av de tre anførte hjemmelsgrunnlagene i §8 foreligger for at behandlingen skal være lovlig.

4.1 Grunnleggende vilkår i personopplysningsloven §8 jf §9

De tre alternative grunnlagene i pol.§8 er samtykke, fastsatt i lov og ”nødvendig”.

De skjerpede kravene for behandling av sensitive opplysninger i pol. §9 kommer dessuten til anvendelse. Herunder tilleggsvilkår i forbindelse med behandling av opplysninger blant annet relatert til mistanke om straffbare handlinger, religiøs oppfatning, etnisk bakgrunn og helsemessige forhold jf pol. §2 nr.8.

Verken G-3/2005 eller KSF 2/2005 oppgir hvilke av hjemmelsgrunnlagene i pol. §§8 og 9 som ligger til grunn for behandlingen i INFOFLYT.

4.1.1 Hjemmelsgrunnlaget "samtykke"

Samtykke som hjemmelsgrunnlag kan det her sees bort fra da "samtykke" etter pol.§2 nr.7 innebærer at det ikke foreligger tvang. De fleste av de registrerte befinner seg i en tvangssituasjon ved å være innsatt i fengsel. Selv om man kan si at de innsatte selv har satt seg i tvangssituasjonen ved å begå kriminelle handlinger, er det uten betydning i forhold til de krav loven stiller til samtykke. Etter §2 nr.7 må samtykket være "uttrykkelig".

De registrerte i INFOFLYT har ikke fått noen forespørsel om å samtykke i behandlingen. I mange tilfeller vil de registrerte heller ikke vite at de er registrert da verken kriminalomsorgen eller politiet gir melding til de berørte.

4.1.2 Hjemmelsgrunnlaget "fastsatt i lov"

Det andre alternative grunnvilkåret for behandling av personopplysninger, er at det er fastsatt i lov.

G-3/2005 inneholder ingen klar anvisning på at det skal eller kan opprettes et eget INFOFLYT-register, hvilket formål registeret skal ha, hvilke typer opplysninger som skal behandles eller hvem som skal omfattes av behandlingen. Retningslinjer og instruks for behandling av opplysninger i INFOFLYT-systemet, overlater departementet til de underordnede forvaltningsorgan KSF, Riksadvokaten, POD og PST å utarbeide.⁵⁹

Riksadvokaten opplyser at embetet ikke har utarbeidet egen saksbehandlingsinstruks, at embetet ikke bruker systemet og heller ikke har gitt uttalelser i forbindelse med høringer annet enn ved tilblivelse av rundskriv og instruks. Disse uttalelsene er unntatt offentligheten jf gamle offentlighetslov §6a og kan i følge Riksadvokaten heller ikke offentliggjøres i dag.⁶⁰

PODs instruks regulerer politiets bruk av INFOFLYT. Instruksen inneholder ingen henvisning til konkret hjemmelsgrunnlag utover å vise til G-3/2005 og en generell henvisning til at "Både politiet og kriminalomsorgen har som formål å forebygge kriminalitet og trygge samfunnet".⁶¹

⁵⁹ G-3/2005 pkt.3

⁶⁰ Riksadvokaten, e-post, februar 2010

⁶¹ POD 2005/00319 pkt.1.1

PST bekrefter i mail at organet ”..har egne regler på dette, som en del av sjefens interne regelverk”. Utover dette kan organet ”..av sikkerhetsmessige årsaker..” ikke gi ytterligere opplysninger om organets behandling av personopplysninger gjennom INFOFLYT.⁶²

I følge KSF 2/2005 er retningslinjene gitt med hjemmel i strgjfl. §§10 og11, forskrift til straffgjennomføringsloven §7-1, departementets rundskriv G-3/2005 og ”øvrige bestemmelser i loven, forskriften og retningslinjene som innebærer sikkerhetsmessige vurderinger”. I instruksjonen heter det videre at KSF skal ha ”et sentralt register over hvem som omfattes av INFOFLYT, med relevante opplysninger om disse”.

Strgjfl. §10 omhandler ulike former for straffgjennomføring og §11 angir vilkårene for bruk av ulike gjennomføringsformer ved innsettelse i fengsel. Etter sin ordlyd er det vanskelig å se at dette gir hjemmel til å gi retningslinjer i rundskrivs form som gir KSF anledning til å opprette et ”sentralt register over hvem som omfattes av INFOFLYT, med relevante opplysninger om disse”.

Sivilombudsmannen har bedt departementet redegjøre nærmere for hjemmelsgrunnlaget angitt i rundskriv KSF 2/2005.⁶³ Departementet oppgir i sitt svarbrev ”..at det ved en inkurie er oppgitt feil hjemmelsgrunnlag..”, og at riktig hjemmelsgrunnlag for rundskrivet er strgjfl. §5(4) og forskrift til strgjfl. §8-1 samt alminnelig instruksjonsmyndighet.⁶⁴ Oppgitte bestemmelser hjemler imidlertid bare at KSF kan gi nærmere retningslinjer for straffgjennomføringsloven og dennes forskrift.

Departementet oppgir videre at ”Opplysningene i INFOFLYT vil etter departementets oppfatning falle inn under personopplysningsloven §8 første ledd og §9 bokstav b, jf strgjfl. §2.”⁶⁵

⁶² PST, e-post, februar 2010

⁶³ Ombudsmannsak 2007/2274

⁶⁴ Departementet, september 2009

⁶⁵ Ibid. pkt.3

Det er noe uklart hva departementet egentlig mener. Jeg tolker imidlertid departementet dit hen at det mener strgjfl. §2 hjemler behandlingen av sensitive personopplysninger.

Spørsmålet er om dette oppfyller lovskravet i pol. §8 jf §9(1) bokstav b.

Straffegjennomføringslovens §2 samt politilovens §2 er formålsbestemmelser.

Slike bestemmelser angir rammene for lovens virkeområde og bærer ofte preg av å være ”fanebestemmelser” som er generelt formulert.

Med ”formålet med straffen” siktes det i strgjfl. §2 til at ”staten kriminaliserer og straffer utvalgte samfunnsskadelige handlinger for å oppnå beskyttelse mot disse, fortrinnsvis ved straffetrusselens og straffens preventive virkninger”.⁶⁶

I forarbeidene til loven forutsetter departementet at hensynet til straffens formål, til samfunnets sikkerhet og det forebyggende aspektet ivaretas i alle beslutninger som tas under straffegjennomføringen. Departementet fastslår at formålsbestemmelsen vil stille store krav til kriminalomsorgens evne til å ”balansere de sikkerhetsmessige hensyn mot hensynet til den enkeltes individuelle behov”.⁶⁷

Straffegjennomføringsloven gir imidlertid ingen uttrykkelig hjemmel for behandling av sensitive personopplysninger. Anvisning til generelle oppgaver som forebygging, etterforskning og å trygge samfunnet er ikke tilstrekkelig når behandlingen er så omfattende og innebærer en kartlegging av den enkeltes liv slik INFOFLYT kan gjøre. Departementet uttaler i forarbeidene til personopplysningsloven at ”Hjemmelskravet er relativt, slik at det krever klarere hjemmel jo større personvernmessig konsekvens behandlingen kan få.”⁶⁸ En lovhjemmel betyr at Stortinget konkret har vurdert den aktuelle behandlingen og funnet den ønskelig og hensiktsmessig.

At departementet i G-3/2005, anser at kriminalomsorgen og politiet er avhengig av behandling av sensitiv personopplysninger i INFOFLYT-systemet for å oppfylle etatenes formål jf. strgjfl. §2 og politil. §2, kan ikke sies å tilfredstille hjemmelskravet.

Behandlingen av personopplysninger må eksplisitt fremgå av særlovgivningen.

⁶⁶ Gyldendal, lovkommentar, strgjfl. §2, note 4

⁶⁷ Ot.prp.nr.5(2000-2001) pkt.5.1.5

⁶⁸ Ot.prp.nr.92(1998-1999)

Straffegjennomføringsloven regulerer gjennomføring av fengselsstraff og varetekt, og inneholder i tillegg enkelte bestemmelser om gjennomføring av strafferettslige særreaksjoner. Det er derfor spesielt vanskelig å se at straffegjennomføringsloven kan hjemle kriminalomsorgens behandling av sensitive opplysninger om personer som verken er innsatte eller domfelte.

4.1.3 Hjemmelsgrunnlaget ”nødvendig”

Det siste alternative vilkåret i pol. §8, er nødvendighetskravet. Det er i første omgang opp til den behandlingsansvarlige å avgjøre om kravet til nødvendighet er tilfredstilt eller ikke. Kravene til nødvendighet er i §8 bokstavene a-f formulert slik at nesten ethvert behandlingsformål kan legitimeres. Dersom det er viktige personvernspørsmål som kan bli berørt i behandlingen, blir det i forarbeidende understreket at personopplysningslovens formålsbestemmelse skal være et moment i tolkningen. Lovens formål, jf §1, er å beskytte den enkelte mot at personvernet krenkes gjennom behandling av personopplysninger og at behandlingen skjer i samsvar med grunnleggende personvern hensyn, ”herunder behovet for personlig integritet, privatlivets fred og tilstrekkelig kvalitet på personopplysninger.” Mye taler for å bruke formålsbestemmelsen aktivt i tilknytning til vurderingen av nødvendighetskriteriet i §8. I henhold til legalitetsprinsippet krever innsamling og annen behandling av personopplysninger, hjemmel i lov dersom innsamlingen anses å være inngripende. I slike tilfeller kan ikke myndighetene vise til nødvendighetsalternativene som ”grunnlag”.⁶⁹

Vilkåret i bokstav a er uaktuelt da det inneholder et samtykkeelement. Bokstav b, for å ”ivareta en rettslig interesse”, er ikke anvendelig. Bokstav c ”for å ivareta den registrertes vitale interesser”, må tolkes strengt og omfatter bare interesser av betydning for den registrertes liv og helse. Alternativet i bokstav d åpner for behandling når det er av ”allmenn interesse”. Bestemmelsen er ment å omfatte arkivering til statistisk og historisk bruk samt i forskningssammenheng.⁷⁰ Heller ikke bokstav e for utøvelse av offentlig

⁶⁹ Gyldendal, lovkommentar, pol.§1, note 1

⁷⁰ Kommentarutgave, personopplysningsloven s.102

myndighet er anvendelig da bestemmelsen er tenkt anvendt i tilfeller der det for eksempel opprettes arkiver som *kan* inneholde personopplysninger, men hvor primæroppgaven ikke er behandling av personopplysninger.⁷¹

Pol. §8 bokstav f oppstiller en slags sekkepost for behandling man ikke har funnet hjemmel for i noen av de øvrige vilkårene. Vilket er at behandling er nødvendig for at den behandlingsansvarlige skal ivareta en berettiget interesse og at hensynet til den registrertes personvern ikke overstiger den interessen. I forarbeidene vektlegges det at hensynet til personverninteressene bør veie tungt.⁷²

Etter min vurdering bør det i en slik avveining også sees hen til hvilke kontrollmuligheter og klageordninger som for øvrig gjelder for den registrerte dersom behandling av sensitive personopplysninger hjemles i den snevre unntaksregelen i pol. §8 bokstav f. Dersom regelverket for øvrig sikrer at den registrertes interesser ivaretas, kan det være større rom for å hjemle behandlingen i bokstav f. Når det gjelder INFOFLYT er imidlertid også kontroll- og klagemulighetene reelt sett så svake at det er tvilsomt om det kan brukes som støtteargument for å anvende nødvendighetsvilkåret.⁷³

4.1.4 Tilleggsvilkår for behandling av sensitive opplysninger

Dersom INFOFLYT skulle anses å tilfredstille hjemmelsvilkåret i pol. §8, må allikevel ett av tilleggsvilkårene i §9 oppfylles for at behandlingen av sensitive opplysninger er lovlig. Tilleggsvilkårene skal være med på å sikre de registrerte mot unødig og usaklig registrering.

Når det gjelder samtykke- og lovsalternativene i §9(1) bokstav a og b, viser jeg til vurderingene i punkt 4.1.2 og 4.1.3. Jeg poengterer imidlertid at kravene til klar hjemmel er strengere når det er *sensitive* opplysninger som behandles. Blant annet må det spesifiseres i hjemmelsgrunnlaget at det nettopp er *sensitive* opplysninger som behandles. I henhold til legalitetsprinsippet kan det skjerpede lovskravet i §9 ikke anses oppfylt.

⁷¹ Ibid. s.103

⁷² Ibid. s.103

⁷³ Se kap.7

Alternativet i bokstav c omhandler behandling som er nødvendig for å beskytte en persons vitale interesser. Bestemmelsen kan tenkes brukt for eksempel for å beskytte informanternes liv. Det er imidlertid et kumulativt vilkår at den registrerte selv ikke kan gi samtykke til behandlingen. Selv om det nødvendigvis ikke trenger å være den registrertes vitale interesser som skal beskyttes, kan det dermed være vanskelig å anvende denne bestemmelsen, iallfall som et generelt grunnlag for INFOFLYT.

Alternativet i bokstav d hjemler behandling av personopplysninger den registrerte frivillig har gjort alminnelig kjent, og bokstav e hjemler behandling for å gjøre gjeldende eller forsvare et rettskrav. Ingen av bestemmelsene er aktuelle for INFOFLYT.

Alternativet i bokstav f omhandler behandling av opplysninger som anses nødvendig for at behandlingsansvarlig skal kunne gjennomføre sine arbeidsrettslige plikter eller rettigheter, for eksempel i forbindelse med innkreving av fagforeningskontingent.⁷⁴

Alternativene i bokstav g og h, nødvendig av helseårsaker og for historisk, statistiske eller vitenskapelige formål er heller ikke anvendelig i forhold til INFOFLYT.

Annet ledd i §9 omhandler sammenslutninger og stiftelser.

Etter dette gjenstår unntaksregelen i §9 siste ledd. Datatilsynet kan ved enkeltvedtak gi tillatelse til at sensitive opplysninger behandles dersom ”viktige samfunnsinteresser” tilsier det. Det er høy terskel for å komme inn under hjemmelen. De tilfellene som kan omfattes, vil oftest være konsesjonspliktige jf pol. § 33.⁷⁵ Kriminalomsorgen har ikke søkt om slik tillatelse.

Behandlinger som har til formål å avdekke visse typer sensitive personopplysninger, typisk straffbare forhold, vil imidlertid kunne anses å ha så stor samfunnsmessig interesse at de vil kunne foretas selv om ingen av vilkårene i §9 foreligger. Dette gjelder for eksempel fjernsynsovervåkning som det derfor er gjort direkte unntak for i loven jf. pol. §37.

Dersom INFOFLYT anses å være av så viktig samfunnsinteresse at behandlingen ikke behøver å oppfylle noen av grunnvilkårene i §8 jf §9, bør behandlingen lovfestes slik at en sikrer at Stortinget har vurdert alle prinsipielle sider av behandlingen.

⁷⁴ Kommentarutgave, personopplysningsloven s.109-110

⁷⁵ Kommentarutgaven, personopplysningsloven s.113

4.2 Formålskravet etter pol. §11 bokstav b og c

Formålet med behandlingen må være saklig begrunnet i den behandlingsansvarliges virksomhet, jf pol. §11 bokstav b. Det oppgitte formålet med INFOFLYT er jf G-3/2005 å forebygge kriminalitet og trygge samfunnet jf strgjfl. §2 og politiloven §2.

Et sentralt vurderingstema når kriminalomsorgen skal foreta beslutninger i enkeltsaker vedrørende innsatte, vil blant annet være faren for at den innsatte skal begå nye straffbare handlinger. Å ta hensyn til samfunnets behov for vern, betyr at kriminalomsorgen alltid skal ha sikkerheten for øye ved slike beslutninger.⁷⁶

Så lenge formålet med behandlingen av INFOFLYT-opplysninger er å foreta riktige sikkerhetsmessige vurderinger, vil behandlingen ligge innenfor kriminalomsorgens naturlige virksomhet. Politiets behandling av personopplysninger i INFOFLYT, faller innenfor formålskravet så langt behandlingen er et ledd i politiets oppgaver jf politiloven §2. Dette betyr ikke at politiet og kriminalomsorgen har full frihet til å behandle, registrere og utveksle enhver type informasjon. Grunnleggende prinsipp i personvernet er at formålet skal angis på en rimelig presis måte.⁷⁷

Etter pol. §11 bokstav c kan personopplysningene ikke uten samtykke fra den registrerte brukes til senere formål som er uforenelige med det opprinnelige formålet med innsamlingen. I INFOFLYT-sammenheng vil det kunne være et spørsmål om politiets formål med innhenting av opplysninger er forenelig med kriminalomsorgens bruk av de samme opplysningene. Dette ser jeg på som et utleveringsspørsmål som behandles i kapittel 5.

⁷⁶ Gyldendal, lovkommentar, strgjfl. §2, note 4

⁷⁷ Personverndirektivet art.6(1)b, rammebeslutningen art.3 nr.1 og 2

4.3 Relevanskravet

En presis formålsangivelse er viktig for å kunne vurdere det fjerde kumulative vilkåret; opplysninger som behandles skal være relevante i forhold til formålet jf pol. §11 bokstav d. De skal også være tilstrekkelige og så fullstendige at de blir representative. Kravet til relevans blir strengere jo mer sensitive opplysningene er.

KSF skal vurdere om opplysninger ut fra sin ”art og alvorlighetsgrad skal registreres i INFOFLYT-registeret”.⁷⁸ Utover dette er det ikke angitt noen avgrensning av hvilke opplysninger kan behandles. Det er ikke angitt hva som er ”alvorlig” nok til at vedkommende havner på INFOFLYT.

INFOFLYT skal være et system for utveksling av informasjon kriminalomsorgen ”trenger for å beslutte riktige sikkerhetsmessige tiltak”.⁷⁹ På bakgrunn av opplysningen skal regionene og fengslene ”beslutte nødvendige tiltak mot de aktuelle personene”.⁸⁰ Nærmere retningslinjer for når INFOFLYT-opplysninger vil være relevante i vurderinger i konkrete saker eller hvilken vektlegging opplysningene skal gis, er ikke gitt.

Hva som er relevant er dermed i stor grad opp til behandlingsansvarliges skjønn og kan dermed kollidere med hensynet til forutsigbarhet og prinsippet om likebehandling som er en viktig kjerneverdi innen kriminalomsorgens virksomhet. Jo vagere regelverket og retningslinjene er på hvilke opplysninger som er relevante, jo større blir skjønnen som utøves. Det betyr igjen at det stilles store krav til den behandlingsansvarlige å påse at skjønnen er innenfor grensene for saklig og forsvarlig saksbehandling. Særlig fordi både Sivilombudsmannen og domstolene er svært tilbakeholdne med å overprøve forvaltningens skjønn.

⁷⁸ KSF 2/2005 pkt.4

⁷⁹ l.c.

⁸⁰ KSF 2/2005 pkt.6

4.4 Krav til opplysningskvalitet og sletting

Etter pol. §11 bokstav e, er det dessuten et grunnkrav at opplysningene som behandles, er korrekte og oppdaterte. Opplysningene skal være relevante og fullstendige i forhold til sine bruksområder.⁸¹ I dette kravet ligger at den behandlingsansvarlige skal etablere tiltak for å sjekke kvaliteten på opplysningene.⁸²

Politiet ved Nye Kripos og PST, er ansvarlig for utformingen av opplysninger som formidles til KSF gjennom INFOFLYT.⁸³ Det presiseres i KSF 2/2005 at ”Når ikke verifiserte opplysninger utleveres, bør det gjøres oppmerksom på at deres korrekthet ikke er avklart.” I PODs instruks punkt 5 står det: ”Når de opplysninger som utleveres ikke er verifiserte, skal det gjøres oppmerksom på dette.” Nye Kripos er videre ansvarlig for kvalitetssikring av informasjonen som formidles til KSF.⁸⁴

Politiet mottar en rekke ikke-verifiserte opplysninger for eksempel fra kilder, informanter og tips fra publikum. Når formålet er lovbestemt, tillates politiet i stor grad å innhente slike opplysninger. I den videre bruken av disse opplysningene, er det imidlertid viktig at det skjer en kvalitetssikring.

Ombudsmannen har uttalt at kriminalomsorgen skal foreta en selvstendig vurdering av INFOFLYT-opplysninger når de inntas som en del av beslutningsgrunnlaget i enkeltsaker. Registrering i INFOFLYT i seg selv, gir i følge ombudsmannen ikke grunnlag for å avslå søknader av sikkerhetsmessige hensyn.⁸⁵

Jeg mener at kriminalomsorgens ansvar jf. pol. §11 bokstav e, strekker lengre enn til å foreta en selvstendig vurdering av opplysninger som brukes som del av beslutningsgrunnlag. Som behandlingsansvarlig har kriminalomsorgen ansvaret for opplysningenes kvalitet i det øyeblikk de *registreres* i INFOFLYT.

⁸¹ Personverndirektivet art.6(1)c

⁸² Pol. §14, personverndirektivet art.6(1)d

⁸³ KSF 2/2005 pkt.5

⁸⁴ POD 2005/00319 pkt.6.1

⁸⁵ Ombudsmannssak 2006/1502

I samtale med tjenestemenn i Nye Kripos, bekreftes det at det gis korrigeret beskjed dersom informasjonen politiet har formidlet via INFOFLYT, viser seg å være feil. Men det fremholdes at i praksis er det sjelden politiet får ”bevis” for at informasjonen er gal og at det dermed sjelden foretas slike korreksjoner.

Følgende eksempel gis: Politiet kan motta informasjon fra tipser eller informant om at en innsatt deltar i planlegging av et ran som skal begås om to måneder. Når tiden er inne, skjer det ingenting. I følge politiet trenger ikke dette bety at informasjonen de fikk var ”feil”. Man vet bare at ranet ikke ble gjennomført, ikke årsaken til det. Ranet kan være utsatt eller andre hindringer har kommet i veien. I slike tilfeller gis det i følge Nye Kripos, ikke kontramelding til KSF. Det betyr at informasjonen i systemet ikke ”tilbakekalles” da det etter politiets oppfatning ”ikke er bevist at informasjonen var feil”.

Eksempelet illustrerer noe av utfordringene med INFOFLYT-systemet. Opplysningene kan jo være feil. De kan ha kommet fra noen som ønsker å skape problemer for den innsatte. Det kan også være at informasjonen som er videreformidlet til politiet og kriminalomsorgen baserer seg på misforståelser. Selv om politiet ikke har bevis for feilinformasjon, har de heller ikke bevis for at det virkelig ble planlagt en kriminell handling som involverte den registrerte.

Der slike opplysninger blir brukt som del av beslutningsgrunnlaget for enkeltsaker, vil den registrerte med all sannsynlighet ikke få innsyn i opplysningene og dermed ikke få mulighet til å forsvare seg mot mistanken. Dette kan være i strid med det grunnleggende rettssikkerhetskravet om retten til kontradiksjon og kan dermed være i strid med uskyldspresumsjonen.

Kriminalomsorg region nord bemerker i ombudsmannssak 2006/1502 at kriminalomsorgen ikke har noe selvstendig etterforskningsapparat som kan verifisere politiets opplysninger, og at opplysningene derfor i stor grad må kunne legges til grunn for kriminalomsorgens avgjørelser. Ombudsmannen mener imidlertid at dette ikke er til hinder for at kriminalomsorgen foretar en selvstendig vurdering og at man kan velge å se bort fra opplysninger som virker lite fundert eller som gjelder forhold som ligger langt tilbake i tid.

I denne sammenheng understreker ombudsmannen at ”INFOFLYT er ment å være et kvalitetssikringssystem og ikke må bidra til å gi legitimitet til ubekreftede opplysninger, rykter og spekulasjoner”.

Polititjenestemenn opplyser at kriminalomsorgen ”absolutt” har mulighet til å henvende seg til politiet for å få utvidede opplysninger om det ønskes. For eksempel for å få utdypning av hvor ”sikre” opplysningene er, få vite mer om hvordan opplysningene har fremkommet, hvor gamle de er osv. Dette gjelder også opplysninger som opprinnelig stammer fra politidistriktene og videreformidles av Nye Kripos. Kriminalomsorgen har også mulighet neste gang de skal bruke opplysningene, til å få en vurdering av om informasjonen fortsatt er aktuell.

I følge politiet er det oftest kriminalomsorgen som tar den første kontakten i INFOFLYT-systemet. Kriminalomsorgen har fått med seg at det er en dom med gjengtilknytning og kontakter politiet for å få en trusselvurdering, bakteppet for dommen, om det er spesielle personer fengselet bør være oppmerksomme på i forbindelse med den innsatte mv. Det kan være at en innsatt er dømt som bakmann i en narkotikasak og det fremgår av dommen at vedkommende var sentral i et miljø. Fengselet lurer på om vedkommende når han blir satt til soning eller underveis i soningen, fortsatt har den rollen. Politiet kan så si til kriminalomsorgen: ”Vi har jo ingen beviser ennå, men alt peker i den retning fordi vi har de og de opplysningene”.

Også i forbindelse med utlevering av slike opplysninger, kan kriminalomsorgen be om bakgrunnsinformasjon, for eksempel om det er enkeltstående opplysninger eller del av et større bilde med opprinnelse i flere kilder osv. Dette betyr at kriminalomsorgen har en viss mulighet til å foreta en selvstendig vurdering av opplysningenes kvalitet.

Minimalitetsprinsippet tilsier at mengden personopplysninger skal begrenses til det som er nødvendig for å realisere formålet ved innsamlingen av opplysningene og den videre behandlingen av dem.⁸⁶ Personopplysningslovens §28 har forbud mot å lagre unødvendige

⁸⁶ Personverndirektivet art.6(1)c og art.7-8, rammebeslutningen art.3 nr.1

personopplysninger. Når opplysningene ikke lenger er nødvendige ut fra formålet, skal de slettes. Dette er et viktig hensyn ved behandling av personopplysninger, jf pol.§11(1) bokstav e. Bestemmelsen innebærer at kriminalomsorgen har en selvstendig plikt til å sørge for at opplysningene er korrekte, oppdaterte og nødvendige. Opplysningene kan ikke lagres helt til de registrerte selv reagerer. Kriminalomsorgen må på eget initiativ, med jevne mellomrom, foreta en vurdering av opplysningene.⁸⁷ Dersom opplysningene ikke innehar tilfredstillende kvalitet, er unøyaktige eller urelevante, skal de enten korrigeres eller fjernes.

KSF 2/2005 angir ingen rutiner for retting og sletting av ufullstendige eller unødvendige opplysninger utover at informasjonen i INFOFLYT-registreret skal ”..slettes/makuleres etter 10 år dersom KSF ikke bestemmer noe annet” og at dokumentene på lokalt og regionalt nivå skal makuleres ved løslatelse.

Innenfor den angitte tidsrammen må personopplysningslovens regler etterkommes. Dette framkommer imidlertid ikke av instruksene. Hvordan de som arbeider med INFOFLYT reelt forholder seg til dette spørsmålet, har ikke vært mulig å bringe på det rene. Verken G-3/2005 eller KSF 2/2005 gir henvisning til at personopplysningslovens regler kommer til anvendelse der instruks og straffegjennomføringsloven er taus.

4.5 Vilkår etter EMK

Det er ikke tilstrekkelig å oppfylle kravene etter norsk intern rett for å kunne behandle personopplysninger. Også kravene etter internasjonale konvensjoner Norge er folkerettslig forpliktet til å etterfølge, må oppfylles. Dersom behandlingen av personopplysninger i INFOFLYT er hjemlet etter norsk intern rett, er det til ingen nytte dersom behandlingen allikevel er i strid med EMK pga forrangsprinsippet.

All behandling av personopplysninger vil kunne utgjøre et inngrep i retten til respekt for privatlivet etter EMK art.8(1). I ”rett til respekt” for privatliv, ligger det først og fremst et

⁸⁷ Kommentarutgave, personopplysningsloven s.122-123

vern mot inngrep fra myndighetenes side.⁸⁸ For at inngrep skal kunne skje, må vilkårene i art.8(2) være oppfylt. Inngrepet må etter dette ha hjemmel i lov, det må være nødvendig i et demokratisk samfunn og det må ivareta relevante formål.

4.5.1 Lovskravet i EMK

Lovskravet i EMK kan ikke likestilles med det internrettslige legalitetsprinsippet. I nasjonal rett innebærer legalitetsprinsippet at inngrepet er forankret i formell lov, noe som ikke er et absolutt krav etter EMK.

EMD har fastslått at uttrykket ”i samsvar med loven” i EMK art.8(2) skal tolkes i lys av generelle prinsipper som er fastslått i tilknytning til den samme formuleringen i art.10(2).⁸⁹ Etter EMDs praksis dekker begrepet ”lov” både skrevne og uskrevne rettsregler og inngrepet må ha grunnlag i formell nasjonal regel. EMD har fastslått at regelen i tillegg må være tilgjengelig og forutberegnelig. Disse to tilleggsvilkårene står over nasjonal rett. Det betyr for det første at reglene må være tilgjengelige for den det gjelder. Videre at den enkelte må få en tilfredstillende angivelse av hvilke regler som gjelder, og reglene må være så presist formulert at den de angår i rimelig grad kan forutse hvilke konsekvenser en handling gir. Etter EMDs praksis gir uttrykket ”i samsvar med loven” dessuten en henvisning til lovens kvalitet. Regelen må være i samsvar med kravet om rettsikkerhet og må gi beskyttelse mot vilkårlige inngrep fra myndighetenes side.⁹⁰

I forhold til INFOFLYT betyr dette at dersom strgjfl. §2 skulle anses å oppfylle kravet om grunnlag i nasjonal lovgivning, må i tillegg kravene om tilgjengelighet og forutberegnelighet være oppfylt for at systemet ikke skal være konvensjonsstridig.

Forskrifter og rundskriv kan altså etter EMDs praksis, oppfylle det utvidede lovskravet i EMK dersom tilleggsvilkårene om tilgjengelighet og forutberegnelighet er oppfylt. Siden strgjfl. §2 er generelt formulert, må tilleggskravene oppfylles gjennom forskrifter eventuelt rundskriv og direktiver. Forskriften til straffegjennomføringsloven gir ingen klarhet for de

⁸⁸ Gyldendal, lovkommentar, EMK art.8(1) note 68

⁸⁹ Silver mot Storbritannia jf Sunday Times mot Storbritannia

⁹⁰ Gyldendal, lovkommentar, EMK art.10(2) note 84

INFOFLYT-registrerte om hvilke regler som gjelder og konsekvenser av brudd på reglene. Spørsmålet er om reguleringen av INFOFLYT i form av instruks gitt som rundskriv av underliggende organ, kan anses å oppfylle kravene til tilgjengelighet og forutberegnelighet.

Departementets rundskriv, G-3/2005, er generelt formulert og gir lite konkret informasjon som er anvendelige for den som berøres av INFOFLYT. Det gis for eksempel ingen konkrete opplysninger om hvem som omfattes, hvilken type informasjon som skal behandles, ingen retningslinjer i forhold til slette-, lagrings- og retterutiner og ingen henvisning til innsyns- og klagerettigheter for de registrerte.

For i det hele tatt å kunne få opplysninger som er i nærheten av å oppfylle kravet til forutberegnelighet, må man kunne ha tilgang til INFOFLYT-instruksene. Det er utarbeidet tre forskjellige instruks i tillegg til departementets rundskriv G-3/2005. PODs og PSTs instruks om INFOFLYT er hemmelige og utilgjengelige både for allmennheten og de berørte.

Etter EMDs praksis er det ikke nok at det eksisterer en rettsregel. Regelen som hjemler inngrepet må være offentliggjort. Hemmelige instruks som er ment å utgjøre hjemmelsgrunnlag for inngrep, vil derfor kunne stride mot kravet i EMK art.8(2).

Domstolen la for eksempel ikke vekt på interne retningslinjer for bruk av romavlytting i Malone-saken⁹¹ fordi disse ikke var tilgjengelige for klageren. Tilsvarende følger av Leander-saken om overvåkning.⁹² EMD åpner imidlertid for en viss grad av adgang til å innskrenke hjemmelens rammer i hemmelige interne instruks dersom lovgivningen er formulert så klart at borgerne kan finne ut om han er i en posisjon som kan gi grunnlag for inngrep.⁹³ Reglene for INFOFLYT kan ikke sies å være klart formulert. PODs og PSTs instruks kan etter EMDs praksis dermed ikke utgjøre en del av hjemmelsgrunnlaget.

KSFs instruks 2/2005 er ugradert. Instruksen gir en viss informasjon om hvem som kan bli omfattet av INFOFLYT. Det er imidlertid høyst tvilsomt om regelverket er så presist

⁹¹ Malone mot Storbritannia

⁹² Leander mot Sverige avsnitt 51

⁹³ NOU 2004:6 pkt.4.3.5 og Malone mot Storbritannia avsnitt 67

beskrevet at det oppfyller kravet til forutberegnelighet. Formålet med registreringen og hvilke typer opplysninger som registreres er i liten grad konkretisert. Instruksen bærer preg av å være utformet som et hjelpemiddel for saksbehandlingen for regionalt og lokalt nivå innen kriminalomsorgen, og ikke med tanke på informasjon til de berørte. Instruksen inneholder ingen beskrivelse av de registrertes rettigheter, snarere tvert i mot. For eksempel slår instruksen fast at den registrerte *ikke* har innsynsrett.⁹⁴ Det beskrives videre hvordan en eventuell innsynsbegjæring til domstolene kan påklages av kriminalomsorgen slik at behandlingstiden tar lang tid, noe som medfører at den reelle muligheten for domstolsprøving er svært liten.

Et annet problem i forhold til EMKs lovskrav, er instruksens tilgjengelighet. Etter EMDs praksis må hjemmelsgrunnlaget være *reelt* tilgjengelig. Hjemmelsgrunnlag er tradisjonelt basert på lover og forskrifter. Ingen av de lovene og forskriftene det vil være naturlig å søke til i sammenheng med innsatte, angir noe som i seg selv er en oppfordring for de berørte å søke videre informasjon om INFOFLYT. Verken kriminalomsorgen eller politiet gir uoppfordret noen informasjon om at registeret eksisterer. Tvert i mot uttrykkes det i samtaler med meg at det ønskes minst mulig offentlighet rundt INFOFLYT og at man ønsker at færrest mulig skal kjenne til systemet.

For å få tilgang til instruksen, må man med andre ord vite at INFOFLYT eksisterer. Videre må man faktisk forstå at man kan være berørt. Når det gjelder ”innsattes personkrets” samt ”risikogruppen” vil trolig de færreste være oppmerksomme på at de risikerer å bli registrert i det særskilte systemet. De vil således ikke ha noen oppfordring til å søke opp verken G-3/2005 eller KSF 2/2005.

Når det gjelder de innsatte, kan man kanskje si at de har større oppfordring til å søke opp slik informasjon dersom de vet om INFOFLYT. Verken rundskrivet eller instruksen er så vidt jeg kjenner til, alminnelig tilgjengelig i fengslene. De fins på internett som innsatte normalt ikke har tilgang til. Rent faktisk er dermed rundskrivet og instruksen vanskelig tilgjengelig for innsatte.

Selv om KSFs instruks er ugradert, må den etter dette allikevel anses vanskelig tilgjengelig.

⁹⁴ Se kap.6

Tilgjengelighetsproblemet kunne kanskje vært løst ved at det i likhet med annen informasjon som gis ved innsettelse til soning, blir delt ut et informasjonsskriv om INFOFLYT. Samme framgangsmåte kunne tenkes overfor innsattes pårørende og besøkende. En slik måte å informere på ville imidlertid ikke løst problematikken i forhold til øvrige personer som risikerer registrering i systemet.

4.5.2 Nødvendighetsvilkåret i EMK

Kumulativt vilkår i art.8 nr.2, er at inngrepet må være ”nødvendig i et demokratisk samfunn av hensyn til den nasjonale sikkerhet, offentlige trygghet eller landets økonomiske velferd for å forebygge uorden eller kriminalitet, for å beskytte helse eller moral, eller for å beskytte andres rettigheter og friheter”.

I nødvendighetsvilkåret ligger et krav om forholdsmessighet og proporsjonalitet. Det vil her være en avveining mellom retten til et privatliv og samfunnets behov for beskyttelse og kriminalitetsbekjempelse.

I kriminalomsorgen skal sikkerhetsarbeidet ikke medføre et unødvendig høyt sikkerhetsnivå. De domfelte skal ikke måtte gjennomføre straffen under strengere forhold eller pålegges andre begrensninger enn det som er nødvendig. Det innebærer at det skal være proporsjonalitet mellom antatt risiko og de sikkerhetstiltak som benyttes. Noe som medfører en vurdering av om risikoen skal aksepteres eller ikke.⁹⁵

Likebehandling er en viktig kjerneverdi for kriminalomsorgens virksomhet. Loven skal sette rammer for kriminalomsorgens maktutøvelse. Det skal føres en ensartet praksis, men samtidig har den enkelte krav på en individuell behandling ut fra risiko for ny kriminalitet og behovet for rehabiliterende tiltak.⁹⁶ Innbakt i rettferdighetsprinsippet ligger et krav om at behandlingsansvarlige skal ta i betraktning de registrertes interesser og rimelige forventninger.

Hvorvidt en behandling av personopplysninger er nødvendig i det enkelte tilfellet, vil alltid bero på en konkret og skjønsmessig vurdering. Det er ikke tilstrekkelig at behandlingen er

⁹⁵ St.meld.nr.37

⁹⁶ l.c.

nyttig eller ønskelig eller at opplysningene er ”kjempe å ha”. De må underlegges en konkret vurdering og rent faktisk være nødvendige.

På området kriminalitetsbekjempelse gir EMD konvensjonsstatene forholdsvis vid skjønnsmargin. Men også her vil kravene være strengere proporsjonalt med hvor inngripende behandlingen er. INFOFLYT-systemet må ikke bli en unnskyldning for å behandle visse grupper annerledes uten at det er knyttet faktisk risiko til dem. Det er selve frihetsberøvelsen som er straffen. Straffegjennomføringen skal ikke være mer tyngende enn nødvendig.

Når registreringen omfatter personer som ”kan ha” eller ”antas å ha” tilknytning til politiske eller religiøse nettverk, får INFOFLYT-systemet en grense også mot rettigheter beskyttet av EMK art.9, 10 og 11 om religionsfrihet, ytringsfrihet og foreningsfriheten. Disse menneskerettighetene er etter EMDs praksis gitt et særlig vern. Allikevel er det ikke gitt noen videre retningslinjer i forhold til kriminalomsorgens behandling av slike personopplysninger utover å angi at INFOFLYT omfatter slik registrering.

Til sammenligning er det i politiregisterlovens §7, inntatt særskilte regler om behandling av sensitive opplysninger som religiøs overbevisning og fagforeningstilhørighet. For disse rettighetene gjelder det etter den nye loven et skjerpet nødvendighetskrav ved at slike opplysninger bare skal behandles dersom det er *strengt nødvendig* for formålet.

Nødvendighetskravet når det gjelder behandling av sensitive opplysninger om personer som verken er innsatte eller dømte, vil etter legalitetsprinsippet være svært strengt. Etter min mening vil kravet grense opp mot at registrering nærmest må anses å være uunnværlig for å oppnå formålet, for at de kan tillates registrert.

Dersom en behandlingen av personopplysninger i INFOFLYT skulle vurderes som ”nødvendig”, kan imidlertid ikke nødvendighetsvilkåret erstatte hjemmelskravet etter EMK. Nødvendighetsvilkåret kommer i tillegg til at inngrepet må være hjemmelskravet.

4.6 Konesjonsspørsmålet

Konesjonsplikten må vurderes særskilt for INFOFLYT da systemet er å anse som et eget nasjonalt register, jf punkt 2.4. Det skal søkes om konesjon fra Datatilsynet for å behandle sensitive personopplysninger, jf pol. §33(1). Konesjonsplikten gjelder ikke dersom behandlingen er hjemlet i egen lov jf §33(4).

Datatilsynet fant at det foreligger konesjonsplikt for Kompis etter pol. §33 så lenge det ikke etableres en lovhjemmel.⁹⁷ Tilsynet mener unntakshjemmelen i §33(4) ikke kommer til anvendelse da straffegjennomføringsloven ikke i tilstrekkelig grad anses å regulerer behandlingen som finner sted. Dersom hjemmelsgrunnlaget ikke anses tilstrekkelig for KOMPIS, kan det heller ikke anses tilstrekkelig for behandlingen i INFOFLYT.

Etter pol. §33(5) kan det imidlertid i forskrifts form, gis unntak fra konesjonsplikten. En slik forskrift foreligger ikke for INFOFLYT.

4.7 Forholdet til ny lovgivning

På bakgrunn av pålegg fra Datatilsynet etter kontrollen av Kompis-systemet, opprettet departementet en arbeidsgruppe med mandat å utrede hjemmelsgrunnlaget for kriminalomsorgens behandling av personopplysninger. Arbeidsgruppens innstilling ligger til grunn for forslaget til endringer i forvaltningsloven og straffegjennomføringsloven.⁹⁸ Det er ikke foreslått en egen hjemmel for INFOFLYT. Det foreslås et nytt kapittel 1a i straffegjennomføringsloven: ”Behandling av personopplysninger i kriminalomsorgen”. I forslaget §4a opplistes hvilke personer kriminalomsorgen kan behandle opplysninger om. ”Risikogruppen” jf KSF 2/2005 pkt.3 er ikke blant de som omtales i lovforslaget. Dette betyr at behandling av personopplysninger iallfall for denne gruppen, fortsatt vil være uhjemlet også dersom endringsforslaget vedtas.

Departementet synes selv usikre på om de foreslåtte endringene vil gi tilstrekkelig hjemmelsgrunnlag for behandlingen i INFOFLYT. I brev av september 2009 til Sivilombudsmannen, skriver departementet: ”Departementet mener det er grunn til å utrede

⁹⁷ Datatilsynet, Kontrollrapport 07/01455, pkt.6.4

⁹⁸ Departementet, høringsforslag jnr.2008/03939

nærmere behovet for særlig lovregulering av INFOFLYT og vil oppnevne et utvalg eller en arbeidsgruppe til å vurdere spørsmålet.”⁹⁹

Kravet til lovhjemmel behøver imidlertid ikke bety annet enn at loven inneholder hjemmel for å gi forskrift om en konkret behandling. ”Poenget er at Stortinget skal ha vurdert en bestemt personopplysningsbehandling og besluttet at behandlingen kan eller skal finne sted.”¹⁰⁰

Det stilles strengere krav til lovhjemmel i henhold til pol. §9 enn til tilsvarende bestemmelse i §8. Det må derfor vektlegges om lovgiver har foretatt en faktisk vurdering av de personvernmessige konsekvenser av behandlingen av *sensitive* opplysninger.¹⁰¹ En generell lovhjemmel som gir kriminalomsorgen anledning til å behandle personopplysninger, kan ikke være nok til å oppfylle de strenge krav til behandlingsgrunnlag en kan lede ut av legalitetsprinsippet.

For øvrig vil man uansett få en vurdering av om en forskrift på dette området vil tilfredstille EMKs tilgjengelighetskrav.

Politiregisterloven som skal erstatte strafferegistreringsloven, vil være en særskilt lov som går foran personopplysningsloven. Enkeltvedtak fattet av KSF kan ikke defineres som ”politisk”, og politiregisterloven vil ikke omfatte kriminalomsorgens bruk av INFOFLYT.

⁹⁹ Ombudsmannsak 2007/2274

¹⁰⁰ Kommentarutgave, personopplysningsloven, s.99

¹⁰¹ Kommentarutgave, personopplysningsloven, s.107

5 Adgang til utveksling av opplysninger mellom kriminalomsorgen og politiet

Hovedregelen er at både kriminalomsorgen og politiet har taushetsplikt om de fleste forhold. Informasjonsutvekslingen må derfor hjemles i ulike unntaksregler.

På straffesaksbehandlingsområdet er taushetsplikten for politiet omfattende og detaljert regulert i straffeprosessloven, særlig §§ 61a-61e og i påtaleinstruksen kapittel 3.

Reglene om taushetsplikt om personopplysninger i straffeprosessloven §§61a flg og forvaltningsloven §§13flg er tilnærmet like.

Når det gjelder politiets behandling av personopplysninger som har kommet til dets kunnskap ved annen virksomhet enn ved behandling av straffesaker, er taushetsplikten regulert i fvl. §§13-13f supplert med politill.§24(3) og (4) jf §24(1). Forvaltningsloven inneholder ikke noen ytringsrett i kriminalitetsforebyggende øyemed, men en slik ytringsrett følger av politiloven §24(4) jf (1). Kriminalomsorgens taushetsplikt er etter gjeldende rett regulert i fvl. §§13-13f.

Taushetspliktsbestemmelsene i de nevnte lover tar utgangspunkt i hvilket formål opplysningene er innhentet til (med unntak av strafferegistreringsloven som tar utgangspunkt i om opplysningene hentes fra ulike registre).

Når man vurderer adgangen til utlevering av personopplysninger, bør det legges vekt på det formål som ligger til grunn for utleveringen. Prinsippet om formålsbestemthet forutsetter at utleveringens formål ikke er uforenelig med formålet som lå til grunn for innsamlingen, med mindre noe annet er bestemt i lov eller i medhold av lov. Et sentralt vurderingsmoment vil være om formålet med behandling av opplysninger endrer karakter gjennom utvekslingen.

5.1 Kriminalomsorgen

I utgangspunktet har alle tjenestemenn i kriminalomsorgen taushetsplikt jf. fvl. §13(1). Unntakene er imidlertid så mange at taushetsplikten i praksis setter få skranker for kriminalomsorgens avgivelse av opplysninger i INFOFLYT-saker, bortsett fra opplysninger som er taushetsbelagt etter lov om helsepersonell.

Etter fvl. §13b(1) nr.2 vil taushetsplikten ikke være til hinder for informasjonsutveksling der ulike organ samarbeider om løsning av saken opplysningene er innhentet for.¹⁰²

Fvl. §13b(1) nr.5 gir generelt unntak fra taushetsplikten for å gi andre forvaltningsorgan opplysninger om en persons forbindelse med organet, om avgjørelser som er truffet og opplysninger som er ”nødvendige for å fremme avgiverorganets oppgaver etter lov, instruks eller oppnevningssgrunnlag”. Utlevering av opplysninger kan være nødvendig får at kriminalomsorgen skal kunne løse sine oppgaver. For eksempel kan det være nødvendig for kriminalomsorgen å gi opplysninger til politiet for å få en vurdering av dem eventuelt få utfyllende opplysninger tilbake, slik at fengslet skal kunne fatte riktige avgjørelser.

Forvaltningsloven gir også unntak fra taushetsplikten ved lovbrudd, anmeldelse og lignende, jf fvl. §13B(1)nr.6. I følge G-3/2005 trenger ikke opplysningene være knyttet til en konkret sak. Mistanke er tilstrekkelig. Dette gjelder særlig opplysninger som har betydning for ro og sikkerhet i fengselet samt annen informasjon som kan ha innvirkning på forholdene i fengselet. Typiske eksempler er informasjon om planlegging av rømninger fra fengselet og forsøk på innsmugling av narkotika.

Kriminalomsorgen har dessuten plikt til å orientere politiet om visse forhold jf strl. §§139 og 172.

Selv om unntakene fra taushetsplikten kan virke forståelige, bør mulighetene for videreformidling av sensitive personopplysninger ikke praktiseres slik at all informasjon *skal* videreformidles. I straffegjennomføringsarbeidet er det sentralt å bidra til mindre framtidig kriminalitet ved individuelle forebyggende tiltak slik at straffen kan ha en

¹⁰² Gyldendal, lovkommentar, fvl. §13b(1)nr.2 note 303

forbedrende virkning.¹⁰³ Dersom kriminalomsorgens ansatte blir en slags lyttepost for politiet, vil dette skade tillitsforholdet som er nødvendig i dette arbeidet. Spesielt vil det kunne motarbeide kontaktbetjentens¹⁰⁴ funksjon som gjennom sin dobbeltrolle får tilgang på svært mange personopplysninger. Betjenten skal på den ene siden gi råd og hjelpe den innsatte med å skrive søknader mv. Samtidig skal kontaktbetjenten ivareta den tradisjonelle vaktrollen. En av hovedfunksjonene til kontaktbetjenten er å motivere og støtte den innsatte under straffegjennomføringen. Dette arbeidet vil vanskeliggjøres dersom den innsatte risikerer at alle opplysninger blir videreformidlet til politiet når vedkommende er på INFOLFYT.

Kriminalomsorgen har for øvrig plikt til å foreta en kvalitetssikring av informasjonen før videreformidling.

5.2 Politiet

Unntakene fra politiets taushetsplikt er i praksis omfattende.

Registeropplysninger kan videreformidles til kriminalomsorgen jf strafferegisterforskriften §11 i.f.

Etter strpl. §61c (1) nr. 2 er det adgang til å gi kriminalomsorgen all informasjon som er innhentet i forbindelse med saken og som kan ha betydning for gjennomføringen av straffereaksjonen, med unntak av opplysninger innhentet gjennom kommunikasjonskontroll. Opplysninger fremkommet gjennom kommunikasjonskontroll kan gis til kriminalomsorgen dersom opplysningene kan brukes til å avverge en straffbar handling som kan medføre fengselsstraff, jf strpl. § 216i(1)bokstav d. Som eksempel nevnes opplysninger om mulige rømning og voldsanvendelse i fengselet eller under frigang.¹⁰⁵

Strprl. §61c (1) nr.5 er videre en spesialbestemmelse som åpner for at politiet kan gi informasjon til kriminalomsorgen når ”formålet er å forebygge lovovertridelser eller å

¹⁰³ St.meld.nr.37 pkt.3.1

¹⁰⁴ En tjenestemann med særlig oppfølgingsansvar overfor den enkelte innsatte

¹⁰⁵ G-3/2005

hindre at virksomheten blir utøvd på uforsvarlig måte”. Dette gjelder for eksempel informasjon som er fremkommet gjennom generell etterretningsvirksomhet eller i tilknytning til etterforskning av andre straffesaker.

Videre er taushetsplikten ikke til hinder for at politiet kan gi kriminalomsorgen opplysninger ”når formålet er å forebygge eller avverge straffbare handlinger” jf politiloven §24 (4) nr.2. Det er tilstrekkelig at slik kommunikasjon anses som hensiktsmessig. For at informasjonsutvekslingen ikke skal anses uforholdsmessig, bør det imidlertid være objektive holdepunkter for at man kan regne med at nye straffbare handlinger av en viss alvorlighet vil bli begått.¹⁰⁶

5.2.1 Kan politiet pålegge kriminalomsorgen taushetsplikt?

I den grad det er anledning for politiet å utlevere registeropplysninger eller opplysninger fra kommunikasjonskontroll til kriminalomsorgen, er taushetsplikten i strafferegistreringsloven §8 og dens forskrift §20 gjeldende for ”offentlige tjenestemenn” og ”andre”. Etter strpl. §216i(1) gjelder taushetsplikten for ”alle”.

Politiet kan videre pålegge enhver i kriminalomsorgen taushetsplikt når det utleveres opplysninger som må holdes hemmelig av hensyn til etterforskningen i saken jf strpl. §61c(2). Taushetsplikt kan også pålegges ved utlevering av opplysninger som det ut fra spannings- og etterretningsvirksomheten er nødvendig å holde hemmelig jf politiloven §24(5) jf (2). Mye av den informasjonen som utveksles gjennom INFOFLYT-systemet, vil nettopp være av slik karakter som nevnt i politil. §24(2).

Selv om politiet vil kunne pålegge kriminalomsorgens tjenestemenn taushetsplikt, vil taushetsplikten normalt sett ikke slå gjennom overfor reglene om partsinnsyn jf fvl. §§18 flg. Polititjenestemenn som arbeider med INFOFLYT, uttrykker i samtale at de er bekymret for at etterretningsopplysninger skal bli kjent for innsatte. Juristene deres skal ha gitt beskjed om at man er ”på utrygg grunn”. Videre sies det at det er en slags ”gentlemens agreement” med KSF om at INFOFLYT-opplysninger ikke skal utleveres, og ”dersom de gjør det, vil vi slutte å gi dem informasjonen.” Det oppgis at hensikten med

¹⁰⁶ Myhrer, pkt.3.5.2

informasjonsutleveringen er å hindre at visse innsatte får permisjon, holdes under spesielle overvåkning mv med kriminalitetforebygning som formål.

Det sies videre at etter hvert som systemet blir bedre kjent og innsynsbegjæringene både til politiet og KSF er økende, jo ”mer diskusjon” blir det mellom politiet og KSF om hvem av organene som skal ”finne begrunnelse for å avslå innsynsbegjæringene”.

Polititjenestemennene uttrykker frustrasjon over situasjonen og sier de har etterlyst et klarere regelverk uten at noe har skjedd.

Dersom opplysningene gir et riktig inntrykk av den reelle situasjonen, er det bekymringsfullt av flere årsaker. På den ene siden kan man få en situasjon hvor kriminalomsorgen får INFOFLYT-opplysninger som de legger vekt på i beslutningsprosessen, *uten* at dette fremgår av vedtaket. I så fall vil man stå overfor en skjult begrunnelse som svekker de registrertes rettssikkerhet. Saksbehandlingen vil da være i strid med det kontradiktoriske prinsipp, og med kravene til begrunnelse av enkeltvedtak jf fvl. §§ 24 og 25.

På den annen side kan man få en situasjon hvor vesentlig informasjon om planlagte rømninger eller opprør mv, ikke videreformidles til kriminalomsorgen fordi politiet frykter at sensitive sider av informasjonen skal gjøres kjent for kriminelle. For eksempel at navn på kilder eller at pågående etterforskning skades, om opplysninger ble kjent.

6 Innsynsrett og informasjonsplikt

Innsynsretten er en grunnleggende forutsetning for å kunne ivareta de registrertes rettigheter. Dersom den registrerte ikke er klar over at det behandles opplysninger om ham, har innsynsretten imidlertid begrenset verdi.

Prinsippet om medbestemmelse innebærer at den registrerte skal kunne ha en viss mulighet til å påvirke behandlingen av opplysninger om seg selv. Den behandlingsansvarlige skal sørge for at behandlingen av personopplysninger er kjent og forståelig for de registrerte. Både innsynsretten og informasjonsplikten sikrer åpenhet og kjennskap til behandlingen, noe som igjen vil sikre forutberegnelighet og ivareta de registrertes rettssikkerhet.¹⁰⁷ Dette betyr at den behandlingsansvarlige skal offentliggjøre elementære detaljer om sine behandlingsoperasjoner og på forespørsel gi nærmere opplysninger.¹⁰⁸

G-3/2005 og KSF 2/2005 har utarbeidet retningslinjer for innsynsretten i INFOFLYT.

Disse tar imidlertid utgangspunkt i reglene for registrerte med partsstatus jf. fvl. §§18 og 19 og strgjfl. §7 bokstav c. Innsynsretten for registrerte som ikke er part i forvaltningssak, er overhodet ikke omhandlet i retningslinjene. Heller ikke informasjonsplikten er omhandlet.

6.1 Informasjonsplikten

Utgangspunktet er at den behandlingsansvarlig av eget tiltak skal kontakte den registrerte for å informere om behandlingen jf pol. §§19 og 20. Informasjonsplikten er uavhengig av om opplysningene samles i et register eller ikke. I denne forbindelse skal de registrerte kunne kreve at opplysninger om dem rettes eller slettes når de er ufullstendige, uriktige eller ulovlige å registrere.¹⁰⁹

¹⁰⁷ NOU 2009:1, pkt.15.1.2

¹⁰⁸ Bl.a. personverndirektivet art.12

¹⁰⁹ Pol. §§27 og 28

Kriminalomsorgen har dessuten plikt til å veilede de med partsstatus, slik at de blir i stand til å ivareta sine rettigheter på best mulig måte, jf fv1. §11.

Kriminalomsorgens internettsider gir generell informasjon til besøkende og innsatte om organets behandling av personopplysninger og personvern. Følgende opplysninger om besøkende innhentes: navn, fødselsnummer, adresse, relasjon til den innsatte samt besøkendes vandelsopplysninger og ”andre relevante opplysninger fra politiet”. Formålet med innhentningen oppgis å være ”å ivareta ro, orden og sikkerhet i fengselet”.¹¹⁰ Formålet med innhenting av opplysninger om den innsatte, oppgis å være for ”å tilrettelegge for en betryggende straffegjennomføring, som sikrer den innsatte tilfredstillende forhold, jf. strgf1. §2”.¹¹¹ Videre vises det kort til personopplysningslovens regler om innsyn, retting og sletting.

Utover at opplysningene ”blir lagret i kriminalomsorgens arkivsystemer”, gis det ingen nærmere beskrivelse av lagringen. INFOFLYT er et så særskilt behandlingssystem at det etter min oppfatning, ikke er dekkende å oppgi at opplysningene lagres i ”kriminalomsorgens arkivsystemer”. Registerets eksistens er ikke allment kjent. Tvert i mot synes det som om både politiet og KSF ønsker at INFOFLYT skal være så lite kjent som mulig noe som uttrykkes direkte i samtaler med polititjenestemenn. KSF gir inntrykk av ønske om hemmelighold ved å ikke besvare spørsmål om INFOFLYT, til tross for flere purringer i løpet av arbeidet med denne avhandlingen.

Informasjonsplikten kommer i en særstilling i forbindelse med utlevering av opplysninger fra et organ til et annet. Politiregisterutvalget mente det er en sentral rettsikkerhets- og personverngaranti at den enkelte blir gjort kjent med utlevering av opplysninger fra politiet til annet organ for at mottakerorgan skal kunne gjennomføre sine oppgaver.¹¹²

Informasjon om at kriminalomsorgen innhenter ”andre relevante opplysninger fra politiet”, kan innebære hva som helst. For de registrerte er det av fundamental betydning å vite

¹¹⁰ Kriminalomsorgen.no, ”Informasjon til besøkende til innsatte i fengsel”

¹¹¹ Kriminalomsorgen.no, ”Informasjon til innsatte om behandling av personopplysninger”

¹¹² NOU 2003:21 kap.16

hvilke spesifikke opplysninger som behandles og hvilke registre som inneholder opplysninger om dem, for at de skal kunne gjøre seg kjent med regelverket og dermed kunne ivareta rettighetene sine.

En annen side ved nettløsningen, er tilgjengeligheten. Det er ikke gitt at besøkende finner fram til de aktuelle nettsidene, og de innsatte har ikke tilgang til internett.

KSF 2/2005 ligger også ute på kriminalomsorgens nettsider. Også her er den reelle tilgjengeligheten et springende punkt. Man må trolig vite om rundskrivets eksistens for å finne det. Dersom man finner fram til det, er det ikke gitt at leseren vil oppfatte at rundskrivet angår dem. Videre gir både tittelen ”Særskilt saksbehandlingsinstruks” og formuleringene i rundskrivet, inntrykk av at det er formulert med tanke på kriminalomsorgens egne organer og ikke med tanke på informasjon til de berørte.

Informasjonsplikten overfor INFOFLYT-registrerte som verken er besøkende eller innsatte, kan uansett ikke anses oppfylt gjennom kriminalomsorgens nettsider.

Dersom nettinformasjonen er den eneste som gis, er dette å anse som brudd på informasjonsplikten jf. pol. §§19 og 20.

Etter straffegjennomføringslovens retningslinjer skal straffegjennomføringsloven, dens forskrifter og retningslinjer være tilgjengelig for alle innsatte.¹¹³ I retningslinjene er INFOFLYT-systemet nevnt en gang på følgende måte: ”Det må også vurderes om det er behov for å be Kriminalomsorgens sentrale forvaltning om opplysninger fra Infoflyt-systemet”.¹¹⁴ En slik generell henvisning til INFOFLYT, setter ikke den innsatte i stand til å forstå at han er registrert i systemet og omfanget av behandlingen av personopplysninger. Hensikten med varslingsplikten som følger av pol. §20 er nettopp at den registrerte skal ha oversikt over behandlingen som gjelder ham selv.

¹¹³ Retningslinjenes pkt.1.5

¹¹⁴ Ibid. pkt.1.8

6.2 Generell og individuell innsynsrett

Lovgivningen stiller krav både til generelt og individuelt innsyn i behandlingen av personopplysninger. Hovedregelen er at generelle opplysninger om hvordan behandlingen av personopplysninger foregår, skal være tilgjengelig for *enhver* som spør jf pol. §18(1). Enhver har rett til å vite hvem som er behandlingsansvarlig, hvilke typer behandling som foretas, hvordan det skjer, hvilket formål behandlingen av opplysninger har, hvilke typer opplysninger som behandles, hvor de hentes fra, om og eventuelt til hvem opplysningene utleveres.

I henhold til pol. §18(2) har den registrerte rett til å få informasjon om samtlige opplysninger registrert på ham/henne. Den individuelle innsynsretten utløses ved at det fins registrerte opplysninger om vedkommende og er ikke avhengig av at personen har partsstatus jf fvl. §2(1)bokstav e. Denne retten er avgjørende for å kunne ivareta andre personvern- og rettssikkerhetsinteresser som kontroll av opplysningskvaliteten og mulighetene for retting, sletting og imøtegåelse. Innsynsretten etter personopplysningsloven supplerer dermed partsinnsynet som følger av fvl. §18.

Reguleringen av innsynsretten i KSF 2/2005 tar utgangspunkt i innsynsretten til de med partsstatus. I instruksene heter det at strgjfl. §7 bokstav c i praksis vil kunne ”avskjære innsyn i de sakene som omfattes av INFOFLYT for innsatte og andre personer som måtte være omtalt i opplysningene (f.eks besøkende, brev- og telefonpartnere).”

En slik generell begrensning er et brudd på pol. §18 både i forhold til personopplysninger som ikke er å anse som saksdokumenter og for personer som ikke er å anse som part.

6.3 Unntak jf pol. §§19(2) og 20(2)

Unntak fra varslingsplikten er gitt i pol. §§19(2), 20(2) og 23.

Pol. §19(2) er lite anvendelig da det forutsettes at den registrerte kjenner til at den konkrete innsamlingen og formålet med behandlingen i INFOFLYT.

I §20(2) er det gitt tre unntak fra varslingsplikten: innsamlingen eller formidlingen er fastsatt i lov, varslingen er umulig eller det er på det rene at den registrerte allerede kjenner informasjonen varselet vil inneholde.

Når det gjelder hjemmelsunntaket §20(2) bokstav a, viser jeg til vurderinger i forhold til lovskravet i kapittel 4.

Unntaket i § 20(2) bokstav b om at varsling anses umulig eller uforholdmessig, er lite anvendelig da antall registrerte i følge KSFs egne tall er så få at det bør være overkommelig å få gitt individuelt varsel.

Det siste unntaket fra varslingsplikt i §20(2), er når den registrerte allerede kjenner til informasjonen varslet skal inneholde. Det er ikke tilstrekkelig at den registrerte kjenner til innsamlingen av personopplysninger dersom han ikke vet om de nærmere omstendighetene rundt innsamlingen. Det er videre et strengt krav at det må ”være på det rene” at den registrerte har slik kunnskap.¹¹⁵ Så lenge den registrerte ikke en gang vet om INFOFLYTs eksistens, langt mindre at han selv er registrert, kan jeg ikke se at unntaksbestemmelsen kan anvendes.

6.4 Unntak etter pol. §23

Verken departementet eller KSF har vurdert hvilke unntaksbestemmelser som eventuelt kommer til anvendelse for unntak fra den generelle innsynsretten og informasjonsplikten, jf pol. §23. Bestemmelsen gir kriminalomsorgen rett, men ikke plikt til å nekte den registrerte innsyn dersom vilkårene er oppfylt. Hver enkelt opplysning må vurderes opp mot unntaksbestemmelsen. Det betyr at selv om enkelte opplysninger i et dokument kan unntas fra innsyn, kan ikke dokumentet som helhet unntas innsyn.

Pol. §23(1) bokstav a hjemler unntak for opplysninger som omhandler rikets sikkerhet og forholdet til fremmede makter mv. Dette vil kunne være aktuelt i PST-saker. Opplysninger bør imidlertid bare unndras innsyn dersom det medfører en faktisk påviselig trussel om opplysningen ble kjent for den registrerte.¹¹⁶

¹¹⁵ Kommentarutgave, personopplysningsloven s.167

¹¹⁶ Kommentarutgave, personopplysningsloven s.176-177

Pol. §23(1) bokstav b gjelder opplysninger ”det er påkrevd å hemmeligholde av hensyn til forebygging, etterforskning, avsløring og rettslig forfølgning av straffbare handlinger”.

Unntaket kan brukes i forbindelse med generell innhenting av informasjon med sikte på å avverge mulige fremtidige straffbare forhold. Forebygging og etterforskning i konkret sak vil følge straffeprosesslovens regler selv om det kan tenkes tilfeller som ikke faller under straffeprosesslovens regler, men allikevel gis unntak. For eksempel hvis det gis informasjon og/eller innsyn i opplysninger til en som selv ikke er kriminell men fins i omgangskretsen, kan man risikere at dette tilflyter de kriminelle som dermed vil forstå at politiet er på sporet av dem.

På den annen side er innsyn ofte den beste måten å få korrigert misvisende opplysninger og få luket bort opplysninger som er helt irrelevante. Kriminelle utfører for eksempel helt vanlige gjøremål som medfører kontakt med ”helt vanlige” personer. Kriminelle har barn, går til tannlege og tar kjøretimer. Politiet kan ha beslaglagt avtalebøker med navn, møtested og avtaletidspunkt som i utgangspunktet oppfattes som mistenkelig. I virkeligheten kan det dreie seg om navn og avtaler med barnehagepersonell, sjåførlærere mv. Det er viktig å få luket bort slike legitime kontakter slik at de ikke registreres i det særskilte INFOFLYT-registeret. Dette gjøres raskest og best gjennom innsyn.

Pol. §23(1) bokstav c gir adgang til å unnta opplysninger det anses utilrådelig at den registrerte får innsyn i av hensyn til vedkommendes helse eller personer som står ham nær. Bestemmelsen skal forstås på samme måte som unntaket i fvL. §19(1) bokstav d.¹¹⁷

Bakgrunnen for at det kan regnes som utilrådelig, er av hensyn til den registrete selv. Hensyn begrunnet i den registrertes forhold til personer som står ham nær må vurderes opp mot den registrertes behov for å kunne forsvare seg i forhold til opplysningene. Av hensyn til forsvarlig saksbehandling er det viktig å få belyst saken fra alle sider.

Taushetspliktunntaket i hjemmelens bokstav d, gjelder ikke overfor den opplysningene gjelder. For at unntaket for interne saksdokumenter jf bokstav e skal komme til anvendelse,

¹¹⁷ Kommentirutgave, personopplysningsloven s.176-177

er det en forutsetning at opplysningene ikke er utlevert til andre og er dermed ikke anvendelig for INFOFLYT.

Vilkårene etter bokstav f er strenge da kravene er at det må være ”åpenbare” og ”grunnleggende” offentlige interesser som tilsier unntaket.¹¹⁸ Forebygging av alvorlige kriminelle handlinger med fare for liv, må kunne sies å være av slik åpenbar offentlig interesse. Men det må foretas en konkret vurdering av kriminalitetens alvorlighetsgrad opp mot ulempen unntaket fra innsynsretten vil føre til for den registrerte.

6.5 Unntak jf strgjfl. §7 bokstav c

Det er hensynet til den enkeltes personvern som ivaretas etter personopplysningsloven. Hensynene bak reglene for partsinnsyn etter forvaltningsloven, er begrunnet i andre forhold, for eksempel i det kontradiktoriske prinsipp. Hovedprinsippet er derfor at partene har krav på å få se og imøtegå alle innlegg, faktiske opplysninger mv. som forvaltningen har fått eller innhentet i saken og som legges til grunn for de vedtak som treffes, jf. fvl. §18. Det følger av strgjfl. §7 at forvaltningslovens regler om partsinnsyn kommer til anvendelse. En innsatt har dermed som hovedregel rett til innsyn i dokumentene som ligger til grunn for vedtak under soning.

Det følger imidlertid av strgjfl. §7 bokstav c at det foreligger hjemmel for å nekte en part innsyn ”i et dokument som inneholder opplysninger som det av hensyn til en annen person må anses utilrådelig at parten får kjennskap til” eller ”dersom innsyn er utilrådelig på grunn av sikkerhetsmessige hensyn, eller av hensyn til etterforskning av straffbare forhold”.

I KSF 2/2005 punkt 8 heter det: ”Pga. opplysningenes sensitive karakter og dermed risiko ved spredning, er det naturlig å ha som utgangspunkt at det ikke må gis innsyn i disse spesielle opplysningene”. Etter gjeldende rett er imidlertid utgangspunktet helt motsatt. Forvaltningens dokumenter er offentlige. Det er eventuelle *unntak* som må begrunnes.

¹¹⁸ Ot.prp.nr.92(1998-1999) kap.16

I sak 2007/264 uttaler ombudsmannen at det ikke er rettslig grunnlag for i rundskrivs form å beslutte at innsyn generelt ikke skal gis i INFOFLYT-dokumenter. Hvert dokument skal i utgangspunktet være gjenstand for en konkret og reell vurdering. Det faktum at et dokument er omfattet av INFOFLYT, er ikke i seg selv et relevant argument for å nekte innsyn. Ombudsmannen påpeker at kriminalomsorgen selv må gjøre seg opp en mening om det er noe i det enkelte dokument som gjør at ”sikkerhetsmessige hensyn” trues ved at den innsatte får innsyn. I en slik skjønnsmessig vurdering mener ombudsmannen det må legges vekt på at INFOFLYT er en særordning for en gruppe innsatte og at overvåkningsregimet de er underlagt, er svært inngripende. Muligheten for kontradiktorisk behandling er av ombudsmannens oppfatning, av stor betydning da informasjonen i systemet synes å ha relativt omfattende konsekvenser for den enkeltes soningsprogresjon. Særlig påpekes det at registrerte opplysninger som kan ha betydning for prøveløslatelse eller andre former for soningsprogresjon, vil være tungtveiende grunner som taler for å gi innsyn.

Sikkerhetsmessige hensyn jf strgf. §7 bokstav c innbefatter ”organisatorisk sikkerhet” som er et legitimt hensyn. Det kan altså nektes innsyn dersom man finner at det vil kunne true kriminalomsorgens organisatoriske sikkerhet om visse innhentings- og oppstillingsmetoder blir kjent. Som argument for å nekte innsyn, oppfyller ikke ”organisatorisk sikkerhet” i seg selv kravet til begrunnelse, men må gis et konkret innhold knyttet til den spesifikke saken. I følge KSFs retningslinjer til straffegjennomføringsloven, har den innsatte heller ikke krav på innsyn dersom det er utilrådelig i forhold til andre domfelte, innsatte eller politiets og/eller kriminalomsorgens kilder. Dette betyr imidlertid ikke at man på generelt grunnlag kan nekte innsyn eventuelt delvis innsyn, men dersom det ikke foretas en konkret vurdering av hvert enkelt dokument, foretas det i realiteten ingen reell vurdering.

Unntakshjemmelen i strgf. §7 bokstav c må sees i sammenheng med bestemmelsens bokstav d, som hjemler at dersom opplysninger er unntatt fra innsyn jf. bokstav c, kan det også gjøres unntak fra kravene til begrunnelse jf fvl. §24.

FNs arbeidsgruppe for vilkårlig frihetsberøvelse uttrykker bekymring for manglende rettsikkerhet ved at den innsatte ikke får vite hvilken informasjon som holdes mot dem

ved vedtak om nektelse av prøveløslatelse eller som beslutningsgrunnlag for vedtak om bruk av isolasjon mv.¹¹⁹ Arbeidsgruppen fremhever at alle former for forvaring og fengsling skal være gjenstand for en effektiv kontroll av kompetent nasjonal myndighet. For å kunne gjennomføre en effektiv kontroll mener arbeidsgruppen at den innsatte har rett til en konkret begrunnelse ved vedtak av denne type.¹²⁰

Norsk senter for menneskerettigheter uttaler i forbindelse med FN-rapporten at sakene ombudsmannen har behandlet, viser at det er vanskelig for de innsatte å imøtegå vedtak basert på INFOFLYT fordi spesifikk begrunnelse for vedtaket utover at vedkommende er på INFOFLYT, ikke gis.¹²¹

Dette betyr at selv om det skulle være gode og legale grunner for å nekte innsyn etter strgf. §7 bokstav c, kan det være at inngrepet sett i sammenheng med bruken av §7 bokstav d, vil være i strid med nasjonale og internasjonale regler.

6.6 Meroffentlighet

Prinsippet om meroffentlighet innebærer at dersom det fins et anvendelig lovfestet unntak, må det foretas en vurdering av om de hensyn som begrunner den aktuelle unntaksbestemmelsen, gjør seg gjeldende i det aktuelle tilfellet som foreligger. Dersom det ikke gjør det, bør det gis innsyn.

Selv om det skulle være lovlig grunnlag for å nekte innsyn i et dokument, har kriminalomsorgen plikt til å vurdere om det kan gis innsyn i deler av dokumentet, gjennom en muntlig gjennomgang eller i form av en generell skriftlig framstilling av hva som framgår av dokumentet.

Eventuelt om det kan gis innsyn gjennom en partsrepresentant mot løfte om taushet, jf kriminalomsorgens veiledning om saksbehandlingsreglene i forvaltningsloven og straffegjennomføringsloven punkt. 3.8. I KSF 2/2005 punkt 8 c, fastslås det at prosessfullmektigen ikke har videre innsynsrett enn sin klient og dermed også er avskåret

¹¹⁹ FN, A/HRC/7/4/Add.2, pkt.89

¹²⁰ Ibid. pkt.90

¹²¹ Menneskerettighetssenteret, mars 2008

fra innsyn etter strgjfl. § 7 bokstav c. En slik regelforståelse medfører at det ikke er noen realitet i ordningen med innsyn for partsrepresentant.

Dersom det er slik at opplysningene som utveksles i INFOFLYT-systemet er av en slik karakter at de som *helhet* bør unndras innsyn, berører dette så grunnleggende rettssikkerhetsprinsipper at det bør lovreguleres.

7 Klage- og kontrollordninger

Gode kontroll- og klageordninger er spesielt viktig for rettssikkerheten til de registrerte når systemet ellers er slik at hjemmelsgrunnlaget for behandlingen er uklart og de registrerte i beste fall bare får begrenset innsyn i avgjørelsene mot dem. Dersom kontroll- og klagemekanismene hadde vært gode, kunne dette til en viss grad oppveie for at rettssikkerhetsgarantiene på andre områder er dårlig ivaretatt.

Verken strafferegistreringsloven eller straffegjennomføringsloven har egne regler for klage. For de med partsstatus kommer forvaltningsloven til anvendelse. Øvrige registrerte er henvist til personopplysningslovens regler.

7.1 Datatilsynet

Datatilsynet skal kontrollere at lover og forskrifter for behandling av personopplysninger følges. Tilsynet har anledning til å drive tilsyn med politiets og kriminalomsorgens behandling av personopplysninger jf pol. §42(3) nr.3. Den registrerte må dermed kunne klage til tilsynet dersom man mener behandlingen i INFOFLYT ikke er i samsvar med personopplysningens regler.

Datatilsynet har hittil verken gjennomført kontroll eller realitetsbehandlet noen klager vedrørende INFOFLYT, men opplyser at ”..vi legger til grunn av Kriminalomsorgen tar med seg lærdommen fra Ila-tilsynet¹²² inn mot andre løsninger”.¹²³

En henvendelse fra en innsatt om fengselets bruk av INFOFLYT, ble av Datatilsynets besvart på denne måte: ”Innledningsvis ønsker Datatilsynet å presisere at det dessverre ikke kan gi noe utfyllende svar på Deres spørsmål, da straffegjennomføringsloven som særskilt lov vil gå foran personopplysningslovens regler. Datatilsynet har heller ingen spesiell

¹²² Datatilsynet, kontrollrapport 07/01455

¹²³ Datatilsynet, mail, 14.01.2010

kompetanse når det gjelder tolkning og anvendelse av straffegjennomføringsloven.”

Avslutningsvis skriver tilsynet at ”...Sivilombudsmannen muligens er rett instans for mer utfyllende svar på Deres spørsmål”.¹²⁴

Datatilsynets svar er underlig med tanke på at det er tilsynet som har ekspertisen på området for lovlig og forsvarlig behandling av personopplysninger.

Straffegjennomføringsloven inneholder ingen spesifikke regler for behandling av sensitive personopplysninger. Behandlingen må derfor følge personopplysningslovens regler, noe som er tilsynets spesialområde.

Datatilsynets tilbakeholdenhet i forhold til INFOFLYT, kan ha sammenheng med tilsynets holdning til kontroll av politiets behandling av personopplysninger. Til tross for at Datatilsynet gjennom flere år har vært sterkt kritisk til etatens behandling, har tilsynet hittil ikke gjennomført noen kontroll. Årsaken er at tilsynet mener det ikke har mulighet til å gjennomføre en reell kontroll på grunn av unntak i forbindelse med straffeprosessloven.¹²⁵

Uavhengig av årsak, viser det ovenstående at det ikke føres tilsyn med INFOFLYT.

Når også Datatilsynet med sin spisskompetanse føler seg på utrygg grunn, kan det være et moment som i seg selv taler for at INFOFLYT-systemet er så spesielt at det bør reguleres i en særskilt lov eller forskrift.

7.2 Klage til overordnet forvaltningsorgan

Enkeltvedtak som er truffet av lokalt eller regionalt nivå, kan påklages til henholdsvis regionalt nivå eller til KSF, jf. fvl. §28. Vedtak kan påklages av de vedtaket gjelder for. Dermed kan også besøkende og andre ha partsstatus og klagerett.

Det er sterkt begrenset hvem som skal ha tilgang til INFOFLYT-systemet.

Tilgangsbegrensning kan være betryggende i forhold til mulighetene for uautorisert

¹²⁴ Datatilsynet, ref. 06/01542-2

¹²⁵ Artikkel, Computerworld 08.02.2008

spredning av sensitive personopplysninger, men kan på den andre side føre til uheldige konsekvenser for klagebehandlingen. Bare 3-4 personer i KSF, 3-4 personer på regionsnivå og 2-4 personer på lokalt nivå vil være involvert i behandlingen av opplysninger i systemet.¹²⁶ Det er KSF som avgjør hvilke opplysninger som skal registreres i INFOFLYT.¹²⁷ Det må bety at det er de 3-4 autoriserte personene i KSF, som foretar denne vurderingen. Opplysningene som registreres i systemet, er dermed allerede i utgangspunktet vurdert av KSF til å være av vesentlig betydning for vurderinger av tiltak mot de registrerte.

I realiteten vil registreringen i seg selv således kunne oppfattes som en føring fra sentralt hold til regionene og fengslene. Det vil være vanskelig for underordnet organ å velge å se bort fra opplysninger som KSF mener må brukes som bakgrunn for vurderinger av innsettelse på avdeling med særlig høyt sikkerhetsnivå, nektelse av permisjon mv. Det står direkte i KSF 2/2005 at ”overordnet organ må kontaktes før ny beslutning tas.”

På denne bakgrunn, mener jeg det vil kunne være et tolkningsspørsmål om det er underordnet eller overordnet organ som treffer vedtaket. Dette har betydning i forhold til vurderingen av om det foretas en reell klagebehandling for INFOFLYT-saker. Det avgjørende vil være hvem som i realiteten er ansvarlig for innholdet i vedtaket.¹²⁸ Pga av tilgangsbegrensningen, kan det være de samme personer som vurderte opplysningene da de ble registrerte, som også skal behandle klagen. Om klagebehandler selv ikke har behandlet de konkrete opplysningene tidligere, vil han trolig sitte svært nær vedkommende.

At et organ får muligheten til å se på saken på nytt, gir organet mulighet til å rette opp eventuelle feil ved saksbehandlingen. Spørsmålet er allikevel om klagebehandler har den nødvendige distanse til saken slik at det foretas en reell klagebehandling som tilfredstiller kravene i fvl. §28. Særlig er det grunn til tvil dersom det som begrunnelse for vedtak bare

¹²⁶ KSF 2/2005 pkt.6

¹²⁷ Ibid pkt.4

¹²⁸ Gyldendal, lovkommentar, fvl.§28 note 723

opplyses at avslag gis på bakgrunn av opplysninger kriminalomsorgen har innhentet fra politiet vedrørende den sikkerhetsmessige vurderingen av saken.

En slik begrunnelse var bakgrunnen for Ombudsmannssak 2006/1502. Den innsatte klaget til ombudsmannen over flere avslag på søknader om permisjon og overføring til overgangsbolig. Politiinformasjon formidlet gjennom INFOFLYT-systemet var sentral i saken. I kriminalomsorgens vedtak etter klage fra den innsatte het det bl.a.:

”Kriminalomsorgen region nord har innhentet opplysninger fra politiet vedrørende den sikkerhetsmessige vurderingen i saken. På bakgrunn av disse opplysningene anser vi det ikke sikkerhetsmessig forsvarlig å innvilge domfelte ordinær permisjon på nåværende tidspunkt. Disse opplysningene er unntatt fra partsinnsyn jf. straffegjennomføringsloven §7 bokstav c. Domfeltes anførsler er vurdert, men kan under henvisning til ovennevnte ikke føre frem. Vedtaket blir således å opprettholde.”

Dette vedtaket viser kjernen av problemet med bruken av INFOFLYT i forhold til de registrertes rettssikkerhet: Inngripende tiltak med stor betydning for soningsprogresjonen foretas med bakgrunn i opplysninger om den innsatte som han selv ikke får innsyn i og dermed ikke kan imøtegå. Dette er i strid med det grunnleggende prinsippet om kontradiksjon. At innsyn heller ikke gis hans prosessfullmektig, svekker rettssikkerheten ytterligere.

7.3 Sivilombudsmannen

Saken kan klages inn for Sivilombudsmannen når den er endelig avgjort i forvaltningen. Ombudsmannen kan imidlertid bare komme med uttalelser og har ikke mulighet til å omgjøre forvaltningsvedtaket eller gi forvaltningen sanksjoner av noen art. Ombudet har taushetsplikt og kan få tilgang til alle sakens dokumenter, men kan ikke foreholde opplysningene til den registrerte uten kriminalomsorgens tillatelse. Mulighetene for kontradiksjon er dermed svært liten.

Sivilombudsmannen har hittil ferdigbehandlet to klager tilknyttet INFOFLYT. Som tidligere beskrevet, kom ombudsmannen i begge sakene med kritiske merknader til

kriminalomsorgens saksbehandling. Mens den ene saken omhandlet permisjonssøknader og overføring til overgangsbolig, omhandlet den andre avslag på innsynsbegjæring fra en innsatt.¹²⁹

Ombudsmannen kritiserte blant annet vedtakenes mangelfulle begrunnelser, manglende selvstendig vurdering fra kriminalomsorgens side vedrørende politiopplysningenes kvalitet, og kritikk av regelforståelsen i forhold til blant annet innsynsreglene.

På bakgrunn av bare to klagesaker, har ombudsmannen opprettet sak av eget tiltak hvor han har bedt departementet om redegjørelse for hjemmelsgrunnlaget, forståelsen av innsynsreglene og redegjørelse for selve behandlingen av personopplysninger.

Selv om Sivilombudsmannen her gjør undersøkelser, er spørsmålet om ordningen tilfredstiller lovens krav om reell klagebehandling.

I begge klagesakene brukte kriminalomsorgen strgf. §7 bokstav c som begrunnelse for å nekte innsyn i beslutningsgrunnlaget for vedtakene. Ombudsmannen påpeker selv i sak 2006/1502 at "Ombudsmannen må være tilbakeholden med å overprøve det skjønnet som kriminalomsorgen utøver i forbindelse med sikkerhetsvurderinger." Det betyr at det ikke foretas en fullstendig klagebehandling gjennom ombudsmannens saksbehandling.

De to sakene illustrerer også et annet problem i forhold til spørsmålet om det foretas en reell klagebehandling, nemlig tidsaspektet.

Sak 2006/1502 gjaldt avslag på søknader om permisjoner fra november 2006. Det fremkommer ikke eksakt dato for avslutning av saken, men av uttalelsen fremkommer det at saksbehandlingen ikke var avsluttet pr oktober 2007.

Sak 2007/264 kom inn i 2007, men er omtalt i ombudsmannens årsmeldingen for 2008. I tillegg til behandlingstiden hos ombudsmannen, kommer den tiden kriminalomsorgen har brukt på saken.

Den lange saksbehandlingstiden vil kunne bety at klagebehandlingen ikke vil ha noen reell betydning for den innsatte. Årsaken til en permisjonssøknad kan for eksempel være å delta i sitt barns bursdagfeiring eller skoleavslutning. På grunn av saksbehandlingstiden vil trolig bursdagen mv forlengst være over når klagen realitetsbehandles. Vedkommende kan dessuten være løslatt før klagen er ferdigbehandlet.

¹²⁹ Ombudsmannssak 2006/1502 og 2007/264

Tidsfaktoren kan også være en av årsakene til at ombudsmannen har mottatt så få klager. Den innsatte ser seg rett og slett ikke tjent med å klage. En annen årsak kan være at den innsatte eller ”den innsattes personkrets” ikke klager av frykt for at det kan ha negativ konsekvens for senere permisjonssøknader mv.

Hvor mange klager kriminalomsorgens har behandlet og som ikke er påklaget videre til ombudsmannen, er uvisst da kriminalomsorgen ikke har besvart forespørsel om dette.

7.4 Retten til effektiv prøving jf EMK art 13

Poenget i artikkel 13 er at man skal kunne få saken sin prøvet ved en nasjonal instans. Administrativ prøvelse er i og for seg tilstrekkelig. Det avgjørende er at prøvingsretten eksisterer og at instansen både skal behandle innholdet av klagen og kunne gi tilfredstillende beskyttelse.¹³⁰

Etter EMK art.13 skal enhver ha rett til en effektiv prøving av inngrepet i privatlivet. Som påpekt tidligere i oppgaven, er muligheten for å kunne hevde sin rett, for det første avhengig av at man vet man har rettighetene. Dernest må man få vite grunnlaget for, eller i alle fall få et visst inntrykk av grunnlaget for inngrepet. Dette betyr at man må få innsyn. Når strgjfl. §7 bokstav c benyttes som grunnlag for vedtak, kan begrunnelsen av vedtaket også begrenses jf. strgjfl. §7 bokstav d. Dette betyr at parten ikke får innsyn.

FNs arbeidsgruppe for vilkårlig frihetsberøvelse og Menneskerettighetssenteret i Norge, er spesielt bekymret for at de registrertes rettigheter i forhold til muligheten for effektiv prøvelse jf EMK art.13, ikke oppfylles på grunn av mangelen på innsyn i beslutningsgrunnlaget.

De fleste, særlig i gruppene ”innsattes personkrets” og ”risikogruppen” vil dessuten ikke vite om INFOFLYT-registreringen og er således avskåret fra å benytte eventuell prøvingsrett. Når heller ingen utfører tilsyn med behandlingen, er det nærliggende å konkludere med at det foreligger krenkelse av art.13.

¹³⁰ Gyldendal, lovkommentar, EMK art.13, note 92

7.5 Retten til adgang til domstolene jf EMK art.6

Spørsmålet er videre om klage- og kontrollordningene ved INFOFLYT-systemet er så vage at det kan medføre en krenkelse også av art.6. Grunnleggende prinsipper for rettferdighet i visse typer sivile saker er fastslått i art.6(1). Ikke bare stilles det krav til behandling av rettssaker, men etter EMDs praksis er det lagt til grunn at den også gir rett til adgang til domstolene ("access to court"). Dette prinsippet ble slått fast i Golder-saken¹³¹ da EMD konstaterte at det var en krenkelse at en innsatt var nektet retten til å kommunisere med advokat for eventuelt å anlegge sak. Videre konstaterte domstolen krenkelse i Airey-saken hvor en kvinne som ønsket separasjon gjennom kompliserte rettsforhandlinger, ble hindret på grunn av ubemidlethet og manglende rettshjelp. Dommen innebærer ikke et generelt krav på rettshjelp, men viser at både rettslige og faktiske hindringer er relevante i vurderingen av om det er krenkelse av konvensjonen.¹³²

Dersom en avgjørelse er truffet administrativt, krever art.6 at en etterfølgende instans har full kompetanse. Forvaltningen innrømmes imidlertid en viss skjønnsmessig myndighet hvor det ikke er nødvendig med fullstendig domstolskontroll.¹³³ Adgangen til domstolene kan begrenses¹³⁴, men synspunktet i EMD er utviklet slik at begrensningene ikke må medføre at det sentrale innholdet i rettigheten svekkes.¹³⁵ Som eksempler på hva som kan regnes som en begrensning av adgangen til domstolene, er i Gyldendals lovkommentar nevnt uklare nasjonale rettsregler. Som typetilfelle nevnes manglende dokumentinnsyn.¹³⁶ Begge de nevnte eksemplene på hva som kan være krenkelse av art.6, slår inn med full tyngde i forhold til INFOFLYT.

¹³¹ Golder mot Storbritannia

¹³² Gyldendal, lovkommentar, EMK art.6(1), note 51

¹³³ Zumtobel mot Østerrike

¹³⁴ Golder mot Storbritannia pkt.34

¹³⁵ Gyldendal, lovkommentar, EMK art.6(1), note 51

¹³⁶ I.c.

8 Sluttkommentarer

At formålet med INFOFLYT er godt og legitimt, er ingen unnskyldning for at nødvendige formelle og reelle rammevilkår mangler. Departementet, politiet og kriminalomsorgen bør stå i fremste rekke når det gjelder å drive sin virksomhet i henhold til nasjonale og internasjonale regler. Med INFOFLYT bommer de på nesten alle områder. I tillegg fortsetter bruken til tross for at departementet i flere år har vært klar over at retningslinjer, rutiner mv ikke er i samsvar med gjeldende rett.

Hjemmelsgrunnlaget er i beste fall uklart. Reglene som er fragmentert og spredd i lovverket, gir ingen god oversikt for de berørte dersom de overhodet forstår at dette angår dem. Bruken av rundskriv hvorav flere er klausulerte, gjør reglene vanskelig tilgjengelig og dersom man finner fram til dem, er de lite konkrete. Det er nærmest umulig for de berørte å forutberegne sin rettsstilling, noe som er kjernen i rettssikkerhetsprinsippet.

Allerede i 2006 etterlyste Sivilombudsmannen nærmere retningslinjer for relevansen og vektleggingen av opplysninger i INFOFLYT-systemet ved avgjørelser av enkeltsaker.

I 2007 påpekte ombudsmannen at det ikke er rettslig grunnlag for å beslutte at innsyn generelt ikke skal gis i INFOFLYT-dokumenter. Kriminalomsorgen opplyste da at KSF 2/2005 skulle revideres.

I januar 2008 leverte Datatilsynet en meget kritisk rapport om kriminalomsorgens behandling av personopplysninger, etter det såkalte Ila-tilsynet. Datatilsynet vurderte det slik at KSF mangler vilje til å etablere rutiner som er i samsvar med personopplysningsloven, og begrunner dette blant annet med at det syv år etter lovens ikrafttredelse ikke var etablert planlagte og systematiske tiltak.¹³⁷ Pr dags dato er det fortsatt ikke etablert fullstendige nye rutiner og system.

FNs arbeidsgruppe leverte sin rapport til norske myndigheter i mars 2008 hvor INFOFLYT ble omtalt som en "issue of concern", og anbefalte tiltak i forhold til rettssikkerheten for de registrerte.

I juni 2009 ba Sivilombudsmannen departementet på nytt om en redegjørelse for arbeidet med revideringen av regelverket. I sitt svarbrev opplyser departementet at det er opprettet

¹³⁷ Datatilsynet, rapport 07/01455

et eget prosjekt for å vurdere hjemmelsgrunnlaget for behandling av opplysninger i kriminalomsorgen generelt, og at et utvalg skal oppnevnes for å vurdere spørsmålet om rettslig grunnlag for INFOFLYT samt øvrige spørsmål tilknyttet systemet. Departementet gjentar i brevet at arbeidet med revidering av KSF 2/2005 pågår.

I forbindelse med denne oppgaven har jeg etterspurt status i revisjonsarbeidet samt utvalgets arbeid. Til tross for purringer, har jeg heller ikke mottatt svar fra KSF om disse spørsmålene.

Mange vil tro at inngrep i forbindelse med INFOFLYT, bare angår innsatte og domfelte, en persongruppe mange trolig mener ikke har spesielle rettigheter. Brudd på norske og internasjonale regler skaper derfor ikke de store overskriftene. Slik oppgaven beskriver, hjemler imidlertid INFOFLYT-instruksene også registrering av personer som aldri har begått kriminelle handlinger samt registrering basert på religiøse og politiske oppfatninger, uten at dette er nærmere regulert.

Dersom Norge ønsker og krever at andre land skal følge menneskerettighetene og ivareta den enkeltes rettssikkerhet, må vi selv følge de forpliktelsene vi har påtatt oss gjennom internasjonale konvensjoner. Ikke bare har Norge plikt til å respektere rettighetene, men staten har en forpliktelse til å sikre dem, jf EMK art. 1. Med det uklare regelverket, mangel på effektiv prøving og manglende dokumentinnsyn, risikerer Norge å få en dom mot seg i EMD dersom noen klager INFOFLYT-systemet inn for domstolen.

Fanger er en gruppe som ikke står høyt i kurs i det brede lag av befolkningen. Kvaliteten på reglene som gjelder for dem vi ikke liker, de utstøtte, er imidlertid selve prøvesteinen for rettsstaten. Etter mine vurderinger, er regelverket for INFOFLYT ikke en rettsstat verdig.

9 Litteraturliste

9.1 Lov

EMK	Europeiske menneskerettighetskonvensjon 21.05 1999 nr. 30
Forvaltningsloven	Lov om behandlingsmåten i forvaltningssaker 10. februar 1967
Menneskerettsloven	Lov om styrking av menneskerettighetenes stilling i norsk rett 21. mai 1999 nr. 30
Ombudsmannsloven	Lov om Stortingets ombudsmann for forvaltningen 22. juni 1962 nr.8
Personopplysningsloven	Lov om behandling av personopplysninger 14. april 2000 nr. 31
Politoloven	Lov om politiet 4. august 1995 nr. 53
SIS	Lov om Schengen informasjonssystem 16. juli 1999 nr. 66
SP	FN-konvensjonen om økonomiske, sosiale og politiske rettigheter 21. mai 1999 nr. 30
Straffegjennomføringsloven	Lov om gjennomføring av straff mv.18. mai 2001 nr.21
Straffeprosessloven	Lov om rettergangsmåten i straffesaker av 22. mai 1981 nr. 25
Strafferegistreringsloven	Lov om strafferegistrering 11. juni 1971 nr. 52
Tvisteloven	Lov om mekling og rettergang i sivile tvister 17. juni 2005 nr. 90

9.2 Forskrifter

Personopplysningsforskriften	Forskrift om behandling av personopplysninger av 15. desember 2000 nr. 1265
Påtaleinstruksen	Forskrift om ordningen av påtalemyndigheten, 28. juni 1985 nr. 1679
Strafferegisterforskriften	Forskrifter om strafferegistrering av 20. desember 1974 nr. 4

9.3 Rundskriv/retningslinjer

Rundskriv G-3/2005	Justis- og politidepartementet ”Informasjonsutveksling mellom kriminalomsorgen og politiet/påtalemyndigheten”
Rundskriv KSF 2/2005	”INFOFLYT – Særskilt saksbehandlingsinstruks”
Rundskriv POD 2005/00319	”Instruks for informasjonsutveksling mellom politiet og kriminalomsorgen i særlig alvorlige saker (INFOFLYT)”
Rundskriv G-111/2000	Justis- og politidepartementet ”Om journalføring og registrering i KOMPIS KIA”.
Retningslinjer	Til lov om gjennomføring av straff og til forskrift av loven, 6. august 2002

9.4 Konvensjoner/direktiv

EØS-avtalen	Avtale om det europeiske samarbeidsområde, ikraft 01.01.94
Personvernkonvensjonen	Europarådets personvernkonvensjon, 28.01.81. nr.108, Convention for the Protection of Individuals with regard to the Automatic Processing for Personal Data

Personverndirektivet	Europaparlaments- og rådsdirektiv 95/46/EF av 24.10.95 om beskyttelse av fysiske personer i forbindelse med personopplysninger og om fri utveksling av slike opplysninger
Rammebeslutningen	Europarådets rammebeslutning 2008/977/JIS av 27.11.08, Om personvern ved behandling av opplysninger i forbindelse med politi- og strafferettsarbeid. Vedtatt i Stortinget 03.12.09.
9.5 Forarbeider	
Fellesorganisasjonen	Høringssvar, Forslag om endringer i forvaltningsloven og straffegjennomføringsloven, 24.06.09
Justis- og politidepartementet	Høring – Forslag om endringer i forvaltningsloven og straffegjennomføringsloven, høringsbrev 28.04.09, jnr. 2008/03939
NOU 1997:19	Et bedre personvern
NOU 2003:21	Kriminalitetsbekjempelse og personvern
NOU 2004:6	Mellom effektivitet og personvern
NOU 2009:1	Individ og integritet
NOU 2009:15	Skjult informasjon – åpen kontroll
Ot.prp.nr. 92 (1998-1999)	Om lov om behandling av personopplysninger
Ot.prp.nr. 5 (2000-2001)	Om lov om gjennomføring av straff mv.
Stortinget dok.nr.15:877(2003-2004)	Skriftlig spørsmål fra Gunn Karin Gjøl (AP), dateret 06.09.2004 besvart av justisminister Odd Einar Dørum 13.09.2004
Stortingsmelding nr.37 (2007-2008)	Straff som virker – mindre kriminalitet – tryggere samfunn

9.6 Rettspraksis

RT. 2000 996

RT. 2005 833

RT. 2006 1409

EMD	Sunday Times mot Storbritannia, 26.04.74 saksnr. 6538/74
EMD	Golder mot Storbritannia, 12.10.74, saksnr. 4451/70
EMD	Silver mot Storbritannia, 25.03.83 saksnr. 5947/72
EMD	Cambell og Fell mot Storbritannia, 28.06.84 saksnr. 7819/1977 og 7878/1977
EMD	Malone mot Storbritannia, 2.08.84 saksnr. 8691/79
EMD	Leander mot Sverige, 26.03.87 saksnr. 9248/81
EMD	Niemietz mot Tyskland, 16.12.92 saksnr. 13710/88
EMD	Zumtobel mot Østerrike, 24.08.93, saksnr. 28/1992/373/447
EMD	Rotaru mot Romania, 04.05 2000 saksnr. 28341/95

9.7 Andre myndigheters praksis

Ombudsmannssak 2006/1502	Kriminalomsorgens bruk av informasjon fra politiet i saker om permisjon og overføring til overgangsbolig
Ombudsmannssak 2007/264	Innsyn i dokumenter i INFOFLYT
Ombudsmannssak 2007/2274	Spørsmål vedrørende INFOFLYT-systemet. Sivilombudsmannens brev til Justis- og politidepartementet av 05.06.2009 samt svarbrev fra Justis- og politidepartementet av 21.09.2009

Datatilsynet, saksnr. 07/01455	Kontroll av behandling av personopplysninger om innsatte i norske fengsler, særlig i det elektroniske informasjonssystemet Kompis, gjennomført på Ila fengsel, forvarings- og sikringsanstalt 13.11.07. Rapportdato: 25. 01.08
Datatilsynet, ref. 06/01542-2	Henvendelse fra innsatt vedrørende INFOFLYT, 13. november 2006
HRC A/HRC/7/4 ADD.2	FNs arbeidsgruppe for vilkårlig frihetsberøvelse, rapport etter besøk i Norge 27.april-2.mai 2007, Report of the Working Group on Arbitrary Detention Mission to Norway A/HRC/7/4 ADD.2, 11.october 2007, framlagt for Utenriksdepartementet 10. mars 2008
NMR	Norsk senter for menneskerettigheter, uttalelse i forbindelse rapporten fra FNs arbeidsgruppe, dato 07.03.08

9.8 Litteratur

Andenæs, Mads Henry	Rettskildelære, Oslo 2009
Bernt/Rasmussen, Frihagen	Forvaltningsrett bind I, Bergen 2003
Gyldendal	Norsk lovkommentar, Oslo 2005
Johansen, Skullerud, Kaspersen	Personopplysningsloven; kommentarutgave, Oslo 2001
Myhrer, Tor-Geir	Politiet og taushetsplikten, Oslo (2000)

9.9 Annet

Computerworld,artikkel	”Datatilsynet: Ingen kontrollerer politiet”, 08.02.08
Datatilsynet	E-post, 14.01.2010
Gyldendal	Norsk lovkommentar, nettutgave, kommentarer til EMK, forvaltningsloven, personopplysningsloven og straffegjennomføringsloven, avlest i perioden 01.02-20.04.10
Kriminalomsorgen.no	”Kriminalomsorgens sentrale datasystem”, http://www.kriminalomsorgen.no/kriminalomsorgens-sentrale-datasystemer.4454702-77856.html (lest 07.04.2010)
Kriminalomsorgen.no	”Informasjon til besøkende til innsatte i fengsel”
Kriminalomsorgen.no	”Informasjon til innsatte om behandling av personopplysninger”
KSF	Årsmelding 2007
KSF	E-post til KSF: 14.01.10, 15.01.2010, 03.02.2010, e-post fra KSF 18.01.2010
Politiets sikkerhetstjeneste	E-post, 12.02.2010
Riksadvokaten	E-post, 18.01.2010
Sivilombudsmannen	Årsmelding 2008
Statistisk sentralbyrå	ssb.no (avlest 01.02.10)

