DET NASJONALE STATSADVOKATEMBETET

FOR BEKJEMPELSE AV ORGANISERT OG ANNEN ALVORLIG KRIMINALITET

Justisdepartementet
Postboks 8005 Dep
0030 Oslo

Deres referanse	*Vår referanse*	*Dato*
200907672 ES KFA/mk	121/09-2	04.05.10

Høring - NOU 2009:15 Skjult informasjon – åpen kontroll:

I. Innledning:

Det vises til departementets brev av 15. desember 2009, med høringsfrist til 1. mai 2010. Videre vises det til e-mail sendt til Knut Hustad hvor det grunnet helt konkrete omstendigheter ble bedt om en kortere fristutsettelse. Det nasjonale statsadvokatembetet (NAST) avgir med dette sin høringsuttalelse til Metodekontrollutvalgets utredning.

Embetet er kjent med Kripos sitt høringssvar datert 19. mai 2010 som er sendt til Politidirektoratet. Embetet finner i det alt vesentlige å kunne tiltre de vurderinger og bemerkninger som Kripos har anført. Vi vil derfor kun kommentere enkelte punkter i utredningen.

Et hovedpoeng for embetet er å peke på de særlige utfordringer som melder seg når norske myndigheter bruker metoder som bistand til andre lands etterforskninger. Dette skjer regelmessig. Utvalget synes ikke å ha drøftet disse problemstillingene særskilt.

Embetet har vurdert metodebehovet i forhold til dagenes situasjon hvor politiet har tilgang til historiske trafikkdata. I embetets saksportefølje er trafikkdata den viktigste etterforskningsmetoden politiet rår over i dag. I disse dager er datalagringsdirektivet ute på høring, og dersom resultatet av den prosessen skulle bli at politiet mister tilgangen til trafikkdata,

Postadresse:	**Kontoradresse:**	**Telefon:**	**Telefax:**
Postboks 8044 Dep 0030 OSLO	Brynsalléen 4 0667 OSLO	23 17 42 00	23 17 42 10

må den øvrige metodetilgangen gjennomgås på nytt og betydelig utvides. Høringssvaret avgis med dette forbeholdet.

Utredningen har to overordnede tema, nemlig politiets bruk av skjulte tvangsmidler, og beskyttelse av informasjon i straffesaker.

II. Skjult tvangsmiddelbruk:

1. Ad: Kap. 14 - Materielle fellesspørsmål

a) Strafferammekravet

Utvalget foreslår å videreføre dagens lovtekniske løsning om at straffebudenes øvre strafferamme er avgjørende for hvilke forbrytelser som gir adgang til skjult tvangsmiddelbruk. Det foreslås ingen endring i det prosessuelle strafferammekravet for metodebruken.

NAST savner imidlertid en vurdering av om dagens krav til strafferammer er hensiktsmessig i lys av det *internasjonale samarbeidsbehovet*, som tilsier at det bør være samme adgang til bruk av skjulte tvangsmidler i Norge som i land man har utstrakt samarbeid med. Embetet arbeider i stor grad med grenseoverskridende kriminalitet. Dette er saker med utstrakt internasjonalt politisamarbeid, og vi ser at det er uheldig at muligheten for tvangsmiddelbruk er forskjellig i de enkelte land. Det vises for eksempel til at i andre land, deriblant Sverige og Danmark, gjelder det en annen strafferamme.

Spørsmålet er viktig ikke bare for effektivt samarbeid, men også for å unngå at kriminelle organisasjoner legger deler av virksomheten til Norge alene fordi terskelen for effektiv metodebruk er høyere her. Utvalget har beskrevet Norges forpliktelse til effektivt internasjonalt samarbeid mot grenseoverskridende kriminalitet (kapittel 8.3, og på s. 101 spalte 2), men har også fremhevet Norges "restriktive regler for inngrep i borgernes rettssfære for å motvirke straffbare handlinger." Utvalget mener at man bør strekke seg svært langt for å opprettholde og videreføre denne "prisverdige tradisjon" (s. 100-101).

På grunn av dagens internasjonale kriminelle modus bør *det internasjonale samarbeidsbehovet* være et sentralt element i avveiningen mellom disse hensyn. Det kan altså være for snevert utelukkende å vurdere hensiktsmessigheten av dagens strafferammekrav innenfor en nasjonal ramme. NAST

reiser derfor spørsmål ved om det burde utføres en sammenlignende undersøkelse av hvor terskelen for skjult tvangsmiddelbruk ligger i Norge, kontra viktige samarbeidsland som Sverige, Danmark, Nederland, Tyskland og de baltiske landene, som grunnlag for en vurdering av om situasjonen er tilfredsstillende.

Norge har bundet seg til flere konvensjoner om politisamarbeid, disse bygger alle på at alvorlig kriminalitet ikke er nasjonale problemer, men utfordringer som må løses gjennom internasjonalt samarbeid. Eksempelvis har vi bundet oss til effektiv bekjempelse og samarbeid gjennom Palermokonvensjonen, vi har harmonisert regelverk gjennom hvitvaskingskonvensjonen og vi er pålagt å kriminalisere nærmere bestemte handlinger som menneskesmugling. En ikke ubetydelig del av NASTs tvangsmiddelbruk skjer som bistand til andre lands myndigheter.

NAST er for øvrig enig med utvalget i at det generelle strafferammekravet suppleres med en liste over andre forbrytelser som etter en konkret vurdering også bør gi grunnlag for bruk av skjulte tvangsmidler. Det vises også til våre merknader om kommunikasjonskontroll i pkt. 4.

b) Overskuddsinformasjon

Embetet støtter også utvalgets forslag om økt mulighet til bruk av overskuddsinformasjon og er enig i den begrunnelse som utvalgets flertall legger til grunn. Av hensyn til effektiv kriminalitetsbekjempelse er det av stor betydning at bevis innhentet på lovlig måte må, som overskuddsinformasjon, kunne benyttes som bevis ved pådømmelse av straffbare handlinger også for forhold som selvstendig ikke kunne begrunne den type kontroll som opplysningene stammer fra.

2. Ad: Kap. 15 - Prosessuelle fellesspørsmål

a) Hastekompetanse

NAST mener det er bra at utvalget ser nødvendigheten av dagens ordning med politiets hastekompetanse, og at det ikke foreslås noen endring her. NAST bekrefter at ordningen er praktisk viktig og støtter utvalgets vurdering. Det vises for øvrig til at det i høringsbrevet om datalagring foreslås ikke å ha en hastekompetanse for innhenting av trafikkdata. NAST har i sin høringsuttalelse til Datalagringsdirektivet påpekt det klare behovet for en slik hastekompetanse. Det er viktig at Samferdselsdepartementet som håndterer datalagringssaken kjenner til Metodekontrollutvalgets klare holdning i dette spørsmål.

b) Samme forsvarer

Utvalget foreslår at samme advokat som hovedregel skal følge behandlingen av begjæringer om skjulte tvangsmidler mot samme mistenkte i en og samme sak. NAST har for så vidt ingen innvendinger mot dette forutsatt at det ikke innføres en absolutt regel. Skjult etterforsking med metodebruk kan strekke seg over år, med begjæringer flere ganger i måneden, og det er ikke realistisk at en og samme advokat vil kunne følge opp hele veien. I tillegg vil det kunne by på uante praktiske problemer i gjennomføringen. NAST viser her til den uttalelse som er utarbeidet av Kripos og støtter de synspunkter som der fremkommer. Embetet vil imidlertid også vise til de forslag som tidligere er lansert om at det til disse formål etableres en gruppe advokater som ikke driver med strafferett og således ikke har de klientene som normalt er de siktede i slike straffesaker. Embetet støtter dette ut fra den mening at selv om den enkelte advokat har en korrekt tilnærming til slike oppgaver, er det ikke alltid like lett å ha en tilstrekkelig oversikt over en stor klientmasse, noe som kan føre til uheldige sammenblandinger.

Det er ikke uproblematisk at en advokat som § 100a forsvarer i sak 1 som gjelder det organiserte kriminelle miljøet x blir kjent med at en person i miljøet er informant. På et senere tidspunkt er advokaten i sak 2 forsvarer for en annen person i miljøet. Informanten er fremdeles aktiv. Dette vil lett skape vanskelige juridiske, etiske og praktiske problemstillinger for advokaten. Det vil videre være tilnærmet umulig for andre å sikre at ikke den konfidensielle informasjon fra sak 1 blir misbrukt på en indirekte måte i sak 2.

c) Innsyn – sakens dokumenter

Utvalget foreslår videre at både advokaten og retten automatisk blir gitt innsyn i hele den foreliggende straffesak, og ikke bare i særlige dokumenter utarbeidet for å begrunne tvangsmiddelet, jf. utvalget uttalelse på side 169. Utvalget forutsetter at slikt innsyn ikke bør være avhengig av en konkret begjæring fra advokaten eller retten, men at saken bør oversendes på samme måte som for en fengslingssak. Begrunnelsen fra utvalgets side er rettens og advokatens mulighet til å utøve en reell kontroll. Hva som menes med dette og hvordan det skal gjennomføres i en operativ skjult etterforskingsfase sier utvalget ingenting om. Etterforskingen i en operativ skjult fase, for eksempel ved bruk av kommunikasjonskontroll, vil ofte være preget av store informasjonsmengder som løpende evalueres og brukes operativt. I den grad noe nedtegnes, vil det ut fra den kunnskap embetet har, normalt skje i form av rapporter ment som grunnlag for begjæringer om skjulte tvangsmidler. Det foreligger således vanligvis ingen ordinær sak ved siden

av den som fremmes for retten i forbindelse med begjæringen. Embetet er ikke uenig i at advokaten og retten skal ha innsyn i sakens dokumenter og ikke bare i "særlige dokumenter utarbeidet for å begrunne tvangsmiddelet" dersom det foreligger dokumenter i saken. Imidlertid er embetet uenig i at dette skal være uavhengig av særlig begjæring fra advokat eller retten. Det må være tilfredsstillende at det gis tilgang dersom det fremsettes begjæring om dette.

d) Oppnevnelse av "§ 100a-forsvarer"

Utvalget foreslår at forsvarer skal oppnevnes etter strpl. § 100a i alle saker om skjult tvangsmiddelbruk. Når det gjelder *skjult fjernsynsovervåking på offentlig sted* vises det til den utvidelse som foreslås i kapittel 21, og NAST er enig i forslaget.

Når det gjelder *teknisk sporing* i medhold av strpl. § 202b, benyttes dette hovedsakelig som et hjelpemiddel ved spaning. Det betyr at *samtidighet* er et viktig kriterium for metodebruken. I dag tilligger kompetansen til å beslutte teknisk sporing etter den nevnte bestemmelsen til påtalemyndigheten. Lovgiver synes å ha ment at metoden hovedsakelig skal brukes sammen med spaning, jf. også at politiet er gitt hastekompetanse til å beslutte teknisk sporing, jf. strpl. § 202b annet ledd.

Forslaget om i stedet å legge beslutningskompetansen til retten med oppnevning av forsvarer etter strpl. § 100a, er derfor en endring som innebærer at det blir vanskelig å iverksette metodene samtidig. Spaning skal jo fortsatt være en operativ politimetode. Dermed bortfaller i stor grad formålet med å kunne bruke teknisk sporing.

Det kan og bemerkes at spørsmålet om beslutningskompetanse for å iverksette teknisk sporing med hjemmel i strpl. § 202b ble drøftet i Ot.prp.nr 64 (1998-1999), og Departementet kom den gang til at det var både forsvarlig og praktisk at kompetansen lå hos påtalemyndigheten i politiet. Dette ut fra forståelsen av at hjelpemiddelet først og fremst ville være et nyttig middel i forbindelse med spaning for å få kontroll på det aktuelle objekt. En slik beslutning må som hovedregel treffes raskt, og det vil kun unntaksvis være tid til forelegge saken for retten på forhånd. Teknisk sporing med hjemmel i §202b må og sies å være et mindre inngripende tvangsmiddel, særlig når det plasseres på gjenstander som for eksempel inneholder narkotika som er det vanligste. Embetet kan ikke se at det er fremkommet vektige argumenter som tilsier at dette bør endres og at beslutningskompetansen bør legges til retten.

NAST går derfor imot dette forslaget, og mener at dagens ordning uansett er tilstrekkelig betryggende. NAST har merket seg at forslaget heller ikke er gjennomført i utvalgets forslag til lovendring s. 369.

e) Muntlig forhandling ved begjæring om skjult tvangsmiddelbruk

Utvalget foreslår at det som hovedregel skal gjennomføres muntlig forhandling ved behandling av begjæring om bruk av skjulte tvangsmidler. Begrunnelsen er at det vil styrke rettssikkerheten.

Utvalgets egen undersøkelse gir imidlertid ikke belegg for at muntlige forhandlinger på dette stadium i strafforfølgingen reelt styrker rettsikkerheten. Det opplyses således at en

> " sammenlikning av disse respondentene med de øvrige respondentene tyder på at praksisen med muntlige forhandlinger i liten grad påvirker utfall og prosess" (s. 171).

Etter NASTs mening ivaretas det reelle behovet av den adgangen det allerede i dag er til å avholde muntlig forhandlinger dersom det antas nødvendig for sakens opplysning.

Selv om ethvert tiltak for å bedre rettssikkerheten i utgangspunktet må vurderes som positivt, må også tiltakets praktiske konsekvenser tas i betraktning. Innføring av en hovedregel om å ha muntlige forhandlinger ved beslutning om hemmelig tvangsmiddelbruk, vil få store ressursmessige konsekvenser. I en operativ etterforskingsfase fremmes det vanligvis et stort antall begjæringer, og muntlige forhandlinger vil medføre en belastning på de som har ansvaret for saken, herunder politi og påtalemyndighet. Særlig vil det binde opp uforholdsmessig mye tid for politiet i en hektisk hverdag. Dertil er det risiko for vidløftiggjøring av behandlingen av begjæringene, noe som forsterkes av uklarheten omkring rekkevidden av innsynsretten i den foreliggende straffesak.

Som en oppsummering savner NAST et dokumentert behov for å snu dagens hovedregel for behandling av slike begjæringer. Siden ulempene kan bli betydelige fremstår det som uklart om målet om bedret rettsikkerhet nås, idet svekket effektivitet i politiets arbeid også har omkostninger for rettssikkerheten. NAST går derfor imot dette forslaget.

Dersom forslaget vedtas, støtter embetet utvalgets forslag om at muntlige forhandlinger kan unnlates når retten finner det klart at slik behandling ikke er nødvendig for sakens opplysning. Utvalget nevner som eksempel at det normalt ikke vil være nødvendig med muntlige forhandlinger der det fremmes ny begjæring fordi den mistenkte bytter telefon. Etter NAST's syn vil det, dersom utvalgets forslag vedtas, normalt være tilstrekkelig med muntlige forhandlinger ved første gangs begjæring om bruk av skjulte tvangsmidler mot en mistenkt. Videre bør det som utgangspunktet ikke være krav om muntlige forhandlinger der begjæring om skjulte tvangsmidler fremmes av utenlandske justismyndigheter via rettsanmodning. I disse saker vil politi og påtalemyndigheter ikke ha ytterligere kjennskap til saken enn det som fremkommer via rettsanmodningen, og saken vil ikke bli bedre opplyst gjennom rettsmøte.

f) Tillatelsens varighet

NAST er enig i utvalgets konklusjon om at det ikke er hensiktsmessig med noen endring i reglene om tillatelsens varighet.

g) Underretning om bruk av tvangsmidler

Utvalget foreslår at dagens regler om utsatt underretning endres slik at mistenkte også ved bruk av kommunikasjonskontroll og romavlytting som hovedregel skal gis underretning ved tvangsmiddelets opphør, og senest når tiltale tas ut eller straffesaken henlegges. Det foreslås mulighet for utsatt underretning for 8 uker av gangen, og for 6 måneder av gangen i saker om overtredelse av straffeloven kapittel 8 eller 9. Utsatt underretning skal ikke kunne gis for alltid, dette gjelder også PST sine forebyggende saker.

NAST viser her til de vurderinger som tidligere er gjort om dette spørsmålet, jf. utredningen s. 174, og kan ikke se at saken står i noen annen stilling i dag. NAST fraråder derfor innføring av ubetinget underrettelsesplikt.

I tillegg vil NAST igjen fremheve hensynet til *internasjonalt justissamarbeid,* og savner en vurdering av hvilke konsekvenser en ubetinget underrettelsesplikt vil få for Norges evne til å delta i dette samarbeidet på tilfredsstillende måte. NAST mottar jevnlig rettsanmodninger fra andre lands justismyndigheter om å innhente tillatelse til bruk av skjulte tvangsmidler.

Det vil også kunne være problematisk å dokumentere behovet for utsatt underretning dersom slik begjæring skal fremmes. Ytterligere er det risiko for at Norge kan bli forhindret fra å bistå dersom reglene i det land som begjærer tvangsmidlet tillater unnlatt underretning i større utstrekning enn etter norsk rett. Det synes klart at dette vil kunne bli hemmende for det internasjonale politisamarbeidet som er nødvendig for effektiv bekjempelse av grenseoverskridende kriminalitet. NAST mener, i likhet med det som er anført vedrørende strafferammekravet for skjulte tvangsmidler (pkt. II.1.a), at det er behov for *sammenlignende undersøkelser* med andre lands rettssystemer, for å påse at norske vilkår er hensiktsmessige i lys av samarbeidsforpliktelsene. Eventuelle endringer i dagens underrettelsesregler bør avventes til en slik undersøkelse er utført.

Et annet praktisk problem er når norsk politi bistår med skjulte tvangsmidler mot en person som er midlertidig i landet, typisk på gjennomreise. En absolutt varslingsplikt av den personen som er i utlandet vil være svært problematisk. En ser for seg en regel om at varsling om tvangsmiddelbruk i bistandssaker overlates til begjærende lands myndigheter. På den måten kan norsk politi gjennomføre bistanden og utkvittere saken. Varsling vil uansett måtte gjennomføres ved at norske myndigheter via rettsanmodning anmoder det land mistenkte befinner seg i, om bistand til å gjennomføre varsling. Hvis de nekter å gjennomføre dette er vi like langt. En kommer således antakelig ikke unna at varsling avhenger av begjærende lands medvirkning. Da kan ansvaret like godt legges der med en gang. En norsk domstols vurdering av vilkårene for fortsatt utsatt varsling vil uansett ikke kunne bli særlig opplyst. Det samme gjelder når vår bistand kreves fordi kommunikasjon av tilfeldige årsaker rutes via Norge. Dette skjer ikke sjelden uten at mistenkte noen gang har befunnet seg på norsk territorium. For norske myndigheter vil det være svært krevende og urimelig byrdefullt å skulle følge opp en slik utenlandsk etterforsking i måneder og år. Det taler med styrke for at varsling overlates til begjærende myndigheter.

3. Ad: Del IV – Behovet for endringer i reglene om skjulte tvangsmidler

a) Generelle bemerkninger

Det hefter noen grunnleggende svakheter ved dagens regelverk som ikke avhjelpes ved utvalgets forslag til endringer i reglene om hemmelig ransaking og kommunikasjonskontroll, herunder forslaget om adgang til å foreta datainnbrudd for å gjennomføre metodene.

Et problem er *lovens skille mellom hemmelig ransaking og kommunikasjonskontroll i lys av den teknologiske utvikling.* Tradisjonelt har ransaking vært knyttet til fysiske rom (og person), mens kommunikasjonskontroll gjelder elektronisk kommunikasjon. Opplysningsgrunnlaget er altså artsforskjellig, nemlig fysiske objekter vs. elektroniske data.

Det har imidlertid lenge vært klart at også datasystemer kan være gjenstand for ransaking, og da er opplysningsgrunnlaget av samme art som ved kommunikasjonskontroll, nemlig elektroniske data. Forskjellen er bare at ved kommunikasjonskontroll er dataene under overføring, mens ved ransaking er de lagret. Hvorvidt dataene bidrar til å opplyse saken, avhenger av om de er tilgjengelige i klartekst. Dersom de er kryptert består informasjonsfangsten bare i uforståelige elektroniske data, og det gjelder både ved ransaking og kommunikasjonskontroll. Bare dersom dataene er dekryptert eller i utgangspunktet er ukryptert, representerer de *informasjon* som kan kaste lys over saken for politiet.

Det kan altså konstateres at teknologiutviklingen har ledet til at ransaking og kommunikasjonskontroll kan rette seg mot samme type objekt (elektroniske data), og kan stå overfor samme utnyttelsesproblem på grunn av kryptering.

Neste aspekt av problemet er den rettslige definisjonen av objektet for kommunikasjonskontroll, nemlig "samtaler eller annen kommunikasjon til og fra bestemte telefoner, datamaskiner eller andre anlegg for elektroniske kommunikasjon", jf. strpl. § 216a tredje ledd. I korthet er det tale om elektronisk kommunikasjon, dvs. data under overføring.

Definisjonen er blitt utbygget i takt med ekomlovgivningen. Det historiske utgangspunktet for kommunikasjonskontroll var at det gjaldt avlytting av samtale mellom *to forskjellige samtaleparter.* At samtalepartene var forskjellige fulgte med nødvendighet av det gamle fasttelefonisystemet, og de strenge vilkår for kommunikasjonskontroll reflekterte følgelig det fundamentale vernet om kommunikasjonsfortroligheten, ikke bare for siktede, men også for den annen part i kommunikasjonen. På grunn av teknologiutviklingen kan ikke forutsetningen om at kommunikasjonen går mellom forskjellige parter opprettholdes bare fordi datastrømmen går mellom forskjellige kommunikasjonsanlegg. Årsaken er at datastrømmen like gjerne kan skyldes personens kontakt med *egne* data som er lagret på en server i "internettskyen". Dermed berøres et annet aspekt av privatlivets fred enn kommunikasjonsfortroligheten.

Det samme gjelder internettbruk som ikke er fortrolig samtale, men kan være bruk av *åpne nettsteder*, for eksempel nyhetstjenester og sosiale medier. Utnyttelsen er basert på bruk av elektroniske kommunikasjonstjenester, men bør neppe anses å være vernet av kommunikasjonsfortroligheten. Spørsmålet gjelder i stedet utstrekningen av vernet om privatlivets fred for handlinger som finner sted i det offentlige rom. Her gir EMK art. 8 bare vern i den grad det gjelder en berettiget forventning om privatliv, et kriterium som skal undergis objektiv fortolkning. Det gjelder neppe en slik forventning ved bruk av tjenester i det offentlige rom, uansett ikke med særlig styrke. Under enhver omstendighet er man ved kommunikasjon med åpent tilgjengelige tjenester *utenfor* de hensyn som begrunner kommunikasjonskontrollreglene, selv om tjenestene ytes ved elektronisk kommunikasjon.

Områdene for kommunikasjonskontroll og ransaking er i ferd med å gli over i hverandre, også fordi det ikke lenger kan legges til grunn at data *ikke* er vernet av kommunikasjonsfortroligheten, bare fordi de er *lagret*. Et velkjent eksempel fra praksis gjelder kriminelle som bruker en epost-konto til å skrive beskjeder til hverandre uten at meldingene sendes. Hver deltaker logger seg inn med brukernavn og passord, og leser de lagrete meldingene. Det er ikke tvilsomt at informasjonsoverføringen representerer kommunikasjon, men metoden som står til rådighet er ikke kommunikasjonskontroll, men ransaking, eventuelt utleveringspålegg overfor tilbyder.

Slik utviklingen går, er det naturlig å anse stadig mer av datamengden som *kommunikasjon*, fordi informasjonen forvaltes i nettverk. For eksempel er det vanlig å forvalte sin informasjon via servere utenfor sin egen personlige datamaskin (kommunikasjonsanlegg). Man er heller ikke avhengig av å disponere en egen datamaskin, fordi informasjonen kan lagres, hentes og spres via servere i "internettskyen" ved bruk av offentlige terminaler, for eksempel på internettkafe eller bibliotek. Videre blir lagrete data ofte (videre)sendt, for eksempel som vedlegg til epost, og representerer derfor kommunikasjon.

Det er neppe gitt hva som er hensiktsmessig eller korrekt metodebruk, kommunikasjonskontroll eller hemmelig ransaking, og politiet vil ende opp med å begjære begge deler for å være på den sikre siden. Kommunikasjonskontroll kan imidlertid være "feil" tvangsmiddel dersom det gjelder en forutsetning om forskjellige samtaleparter. Ransaking er på den annen side utilstrekkelig dersom det ikke er adgang til *regelmessig nedlasting* fra brukerkontoen, slik at politiet kan følge med på informasjonsutvekslingen. Så vidt forstås er gjeldende lære at ransakingsbestemmelsen i

strpl. § 200a ikke gir adgang til dette. Tolkningen følger ikke eksplisitt av ordlyden, men viser vel at konseptet "ransaking" er forankret i åpen metodebruk i det fysiske rom. I slike tilfeller har det ikke vært behov for ransaking flere ganger under samme tillatelse, fordi siktede alt første gang ble gjort oppmerksom på etterforskingsskrittet og har kunnet innrette seg deretter. Men ved hemmelig metodebruk er gjentatt ransaking hensiktsmessig, *både* for fysiske og virtuelle rom.

Her ligger i realiteten tre poenger: For det første at teknologiutviklingen leder til at et rettslig skille mellom lagrede data og data under overføring blir kunstig, slik at lovgiver burde vurdere å lage *én dekkende regel for hemmelig tilgang til elektroniske data.* For det andre at det bør være adgang til gjentatt hemmelig ransaking, både fysisk og virtuelt. Og for det tredje, at når ransaking utføres over nett – altså virtuelt – innebærer det bruk av dataprogram, dvs. en automatisert ransakingsprosess, noe som i seg selv tilsier at det bør være adgang til gjentatt automatisert ransaking.

Et annet problem gjelder den *lovgivningsteknikk* som anvendes for å gi politiet adgang til å utnytte opplysninger for et annet formål enn det metoden opprinnelig var ment for. Dette gjelder i første rekke utbyggingen av reglene om kommunikasjonskontroll til å omfatte identifisering av kommunikasjonsanlegg, og videre til å utnytte elektronisk kommunikasjon for å fastlegge den geografiske posisjonen til kommunikasjonsanlegget, og nå også til personen som bærer kommunikasjonsanlegget, jf. utredningen kapittel 16.6.

NAST støtter selvfølgelig forslaget om at reglene skal tilrettelegge for lokalisering av person, på grunn av det åpenbare behovet for dette. Men det synes å hefte svakheter ved at lovgiver mener det er påkrevet å regulere skritt for skritt hva som skal være *formålet* med informasjonsfangsten, og gjør det i tilknytning til *eksisterende spesifikke metoder*, i dette tilfellet kommunikasjonskontroll.

I dag, med utstrakt bruk av mobil trådløs kommunikasjonsteknologi, er det nokså selvsagt at opplysninger om elektronisk kommunikasjon (metadata) sier noe om *hvor* et kommunikasjonsanlegg er, og følgelig også noe om hvor en person er når anlegget brukes. Men slike opplysninger får en ikke bare ved å utnytte teknologi i forhold til kommunikasjonskontroll, det gjelder også for lagrede data. Ved IP-sporing kan man avdekke *den geografiske posisjonen* til en mistenkt på det tidspunkt vedkommende koblet seg opp til sin brukerkonto i nettet. Og dersom politiet har sendt et rapporteringsprogram til kontoen, kan det gi *varsel* til politiet når oppkobling skjer, slik at tilslag, f.eks. med tanke på pågripelse, kan skje.

Det relevante skillet synes å gå mellom *aktiv og passiv* anskaffelse av lokaliseringsdata. Med "aktiv" menes at politiet anskaffer dataene på egen hånd, og man er da i praksis henvist til bruk av teknisk utstyr av fysisk art som en IMSI-catcher, eller tjenester som politiet anvender selv, for eksempel bruk av et rapporteringsprogram som nevnt, eller som kjøpes av en tilbyder, for eksempel "silent SMS". Den "passive" metoden gjelder utlevering av trafikk- og lokaliseringsdata m.v. fra tilbyder. Også slike data sier noe om posisjon, men er registrert som ledd i vanlig tjenesteyting.

For å oppsummere: (i) Det vesentlige poenget i forhold til lovgivningsteknikken, er at man bør frigjøre seg fra forutsetningen om at metoden enten gjelder data som er lagret eller er under kommunikasjon. Lovgiver bør i stedet overveie å innføre *generelle regler* for utnyttelse av *innholdet* i elektroniske data, og opplysninger om *bruken* av de tjenester som *lagrer og overfører* data.

(ii) Det bør også etableres et mer *dynamisk konsept for hemmelig ransaking,* som tillater gjentatt ransaking mot samme rom/brukerkonto/server, innenfor en bestemt tidsperiode. For hemmelig fysisk ransaking foreligger det for eksempel behov i terrorsaker å kontrollere et rom som politiet vet at brukes for oppbevaring av komponenter til å fremstille en bombe. Trafikk inn/ut av rommet kan bety at flere komponenter tilføres med tanke på endelig fremstilling av bomben, eller at komponentene flyttes til et annet sted for å foreta fremstillingen der. Dette kan ikke avdekkes annet enn ved fysisk observasjon ved ransaking, hvis de impliserte er forsiktige med hva som sies slik at romavlytting er utilstrekkelig. Det kan også vises til et lignende eksempel om overlevering av narkotika i høringsuttalelsen til Kripos nederst på s. 16.

(iii) Ytterligere bør det for virtuelle rom avklares at det er adgang til å utføre gjentatt ransaking automatisert og gjentatt innenfor den perioden som tillatelsen gjelder, simpelthen fordi bruken av virtuelle tjenester er annerledes og krever hyppigere – i praksis automatiserte - undersøkelser, enn ransaking av fysiske rom. Selv om det ikke kan ses at ordlyden i gjeldende ransakingsregler er til hinder for hemmelig gjentatt ransaking, fysisk og virtuelt, hersker det en usikkerhet som påkaller behov for rettslig avklaring.

(iv) Den foreslåtte regelen om identifikasjon og lokalisering av person som bruker elektronisk kommunikasjon, synes dessuten systematisk å høre hjemme i kapitlet om *teknisk sporing*, og ikke

strpl. § 216bb bokstav e, slik det nå står (se utredningen kapittel 16.6 og forslaget til lovendring på s, 371).

b) Ad: Utvalgets forslag om dataavlesing

Metodekontrollutvalget foreslår å tillate dataavlesing for å kunne gjennomføre hemmelig ransaking og kommunikasjonskontroll, men vender tommelen ned for å innføre dataavlesing som selvstendig metode som registrerer den løpende aktiviteten på en datamaskin.

NAST har problem med å forstå utvalgets begrunnelse for å innføre dataavlesing i form av adgang til å foreta datainnbrudd for å foreta kommunikasjonskontroll, jf. forslag til nytt femte ledd i strpl. § 216a. Kommunikasjonskontroll utføres vanligvis med bistand fra tilbyder, en situasjon som ikke gir behov for å begå datainnbrudd for å gjennomføre tilegnelsen av innholdsdata. Dersom kommunikasjonen er kryptert er det imidlertid behov for å få tilgang til *dekrypteringsnøkler* fra tilbyder, slik at kommunikasjonen kan konverteres til klartekst. Slik forslaget til strpl. 216a nest siste ledd er utformet, omfattes ikke denne situasjonen, jf. at det gir tillatelse til "å foreta innbrudd i et datasystem", noe som strengt tatt ikke gjelder kommunikasjonskontroll, men ransaking. Det burde imidlertid fremgå av loven at tillatelse til kommunikasjonskontroll med bistand fra tilbyder *gir politiet rett til å motta kommunikasjonen i klartekst dersom tilbyder er i stand til å dekode innholdet.*

NAST mener uansett at dataavlesing bør innføres som selvstendig metode og ser altså ikke at det er mer integritetskrenkende enn for eksempel kommunikasjonskontroll, som er tillatt. Det er behov for metoden for å fange opp dekrypteringsnøkler, slik at politiet kan utnytte kryptert informasjonsfangst uavhengig av om den stammer fra data som er lagret eller som har vært innhentet ved kommunikasjonskontroll.

Metodekontrollutvalget har tatt utgangspunkt i at metodene skal møte etterforskingsbehovet stilt overfor

> "miljøer preget av elementer som sterk intern justis, profesjonalitet, organisering, mobilitet og internasjonale kontakter." (utredningen s. 110).

Utgangspunktet er altså mennesker i bevegelse, flere som samarbeider og følgelig utnytter elektroniske kommunikasjonstjenester, profesjonelle som vet å beskytte kommunikasjonen ved kryptering.

Hvis lovens formål er å gi politiet mulighet til å følge med på kommunikasjonen mellom kriminelle, er det både behov for kommunikasjonskontroll som i dag, og for gjentatt hemmelig ransaking som kan følge med på en epostkonto eller annen brukerkonto i nettet. Metodene dekker samme formål. Utvalget har drøftet *gjentatt ransaking* under merkelappen "dataavlesing" og kommet til at man ikke vil anbefale metoden,

> "fordi det vil gi politiet anledning til systematisk å kartlegge mistenktes bruk av et datasystem over tid, herunder opplysninger som ikke blir lagret i datasystemet og dermed ikke vil kunne hentes ut ved tradisjonell hemmelig ransaking. Etter utvalgets syn innebærer dette en for stor integritetskrenkelse i forhold til det anførte behovet." (s. 246).

Første del av begrunnelsen er ikke lett å forstå sammenlignet med at man aksepterer bruk av kommunikasjonskontroll. Det ville gitt bedre sammenheng i regelverket om utvalget hadde utformet en *ransakingsregel som ga politiet adgang til foreta informasjonsinnhenting fra brukerkontoen/datasystemet et ubegrenset antall ganger, også med bruk av dataprogram som automatisk rapporterer om endringer, innenfor en nærmere bestemt tidsperiode.*

Andre del av begrunnelsen i sitatet gjelder data som ikke blir lagret, noe som i praksis er passord for tilgang og dekryptering. At dette er nødvendige data for politiet også for *enkeltstående* tilfeller av ransaking, bør være hevet over tvil, så også denne delen av begrunnelsen er vanskelig å forstå. Det er følgelig behov for å utnytte automatiske metoder for *å kopiere lagret innhold og rapportere om bruk av datamaskinen (tastetrykk), samt å kopiere trafikk mellom kommunikasjonsanlegg,* og alt dette bør reguleres i samme bestemmelse.

c) Teknisk sporing

Videre bør regler som gjelder lokalisering av personer, kommunikasjonsanlegg og andre gjenstander som biler etc., reguleres under ett i et kapittel om *teknisk sporing,* hvor reglene gjøres uavhengig av hvilken metode som anvendes rent teknisk.

d) Identifikator for kommunikasjonskontroll og for virtuell ransaking

For så vidt gjelder *kommunikasjonskontroll* bør ordlyden i strpl. § 216a tredje ledd endres slik at tillatelsen ikke bare kan knyttes til et fysisk kommunikasjonsanlegg, men til en bestemt kommunikasjons*tjeneste*, dvs. at det bør følge klart av ordlyden at tillatelsen kan kobles til *en brukerkonto*. Poenget er fint fremhevet av Kripos som skriver at

> "det er vesentlig å ha en lovgivning som ikke begrenses av spesifikasjoner i lovteksten som utelukker kontroll av ønsket kommunikasjon." (Kripos sitt høringsbrev s. 7 nederst).

Poenget er at ett og samme fysiske anlegg kan ha flere brukerkontoer, og det kan være aktuelt å avlytte trafikken dem imellom, for eksempel mellom epostkonti på samme server. Mens en IP-adresse kan tilhøre serveren, identifiserer brukernavnet kontoen. Dermed bør brukernavnet være tilstrekkelig kriterium, og man taler da om bruk av en tjeneste, ikke et bestemt anlegg. I realiteten kan tilbyderen bytte anlegg (server) uten at det påvirker bruken, og politiets metoder må følge *kontoen*, ikke hvorfra den fysisk leveres til enhver tid.

Det samme gjør seg selvfølgelig gjeldende for ransaking over nett (virtuell ransaking). Også her bør tillatelsen knyttes til brukerkonto, fordi de lagrede data kan bli flyttet mellom servere i "internettskyen" uten at brukeradgangen påvirkes. Da bør ikke ransakingsadgangen være begrenset til servere med fysiske identifikatorer. Denne bemerkningen for virtuell ransaking gjelder under forutsetning at tvangsmiddelet for utnyttelse av elektronisk kommunikasjon blir det samme, uavhengig av om dataene er lagret eller er under overføring. Dersom man fortsatt skal basere seg på bruk av strpl. § 192, for ransaking over nett, setter den for så vidt ikke de samme begrensninger som strpl. § 216a gjør med hensyn til identifikasjonen av "kommunikasjonsanlegget". Men dersom reglene endres slik at de tar hensyn til samordningsbehovet mellom metodene, synes identifikatorene for virtuell ransaking å måtte være like fleksible som for kommunikasjonskontroll.

4. Spesielle kommentarer om kommunikasjonskontroll (kapittel 16)

a) Organisert menneskesmugling

NAST støtter utvalgets forslag om å tilføye organisert menneskesmugling, jf. ny bestemmelse i utl. § 108, femte ledd, som et forhold som kan gi grunnlag for kommunikasjonskontroll. Det vises til utvalgets forslag s. 188, og begrunnelsen på sidene forut.

Norge er et av få land i Vest-Europa som ikke har denne muligheten, og behovet synes å være på det rene. Også hensynet til *internasjonalt politisamarbeid* taler for at det innføres adgang til kommunikasjonskontroll for denne type overtredelser.

b) Organiserte utenlandske vinningskriminelle strl. § 162 c

Norge har i dag et stort kriminalitetsproblem med vinningskriminelle bander fra utlandet, særlig Øst-Europa. I enkelte tilfeller blir norsk politi varslet om disse fra utenlandsk politi, typisk at banden er på vei mot Norge fra landet "X". Hvis meldingen fra utlandet kun omfatter grove tyverier, vil ikke norsk politi ha mulighet for kommunikasjonskontroll før de mistenkte krysser forsøkets nedre grense på grovt tyveri, jf. strl §§ 258, jf. 257, jf. § 60 a. Etterforskingsmetoden kan dermed ikke tas i bruk før på et senere stadium hvor de kriminelle er godt i gang med det første grove tyveriet.

NAST foreslår derfor at det også åpnes for kommunikasjonskontroll ved overtredelse av strl. § 162 c, forbund om å begå en straffbar handling med minst 3 års strafferamme som ledd i virksomheten til en organisert kriminell gruppe. Det vil si at strl. § 162 c tilføyes blant de spesielle bestemmelsene i strpl. § 216a første ledd litra b. Bestemmelsen må antas å ville bli brukt bare i et meget lite antall saker, men til gjengjeld vil det foreligge et klart behov for å iverksette kommunikasjonskontroll i slike tilfeller, ved varsel fra utenlandske samarbeidspartnere om vinningskriminelle bander på vei mot Norge. Ved å medta strl. § 162 c, gis det mulighet for å ramme en handling som er ment å eskalere inn til noe større, og det må anses som en ubetinget fordel at politiet kan komme tidlig inn for å hindre at privatpersoner blir utsatt for organisert kriminalitet. Da er det viktig å ha muligheten til å avlytte de kriminelle fra de tar sitt første steg på norsk jord.

III. Beskyttelse av informasjon i straffesaker

Ad: Kap. 26 Dokumentinnsyn

a) Innledning

Det vises til utvalgets gjennomgang av rettsutviklingen og gjeldende rett på området. NAST ønsker å understreke påtalemyndighetens behov for å kunne holde sensitiv informasjon borte fra mistenkte, og ikke minst, behovet for at reglene om dokumentinnsyn i størst mulig grad skaper *forutberegnelighet* på dette punkt.

Som utvalget gjør rede for har rettstilstanden etter Rt. 2007 s. 1435, 2008 s. 1053, 1575 og 2009 s. 1075 utviklet seg til å avgjøre hva som er sakens dokumenter ut fra et saklig tilknytningskrav. Dokumenter som er blitt til eller fremkommet under etterforskingen av saken er følgelig sakens dokumenter.

Som et utgangspunkt er NAST enig med utvalget i at "dokument" er et så innarbeidet begrep at det kan beholdes. NAST deler også utvalgets mål om å skape et klarere regelverk og sikre at dokumenter som bør kunne unntas fra innsyn, blir det. NAST mener imidlertid at utvalgets flertallsforslag har svakheter og at mindretallsvotumet fra utvalgsmedlem *Schea* ikke bare er en vesentlig bedre løsning, men den eneste som i praksis er egnet til å ivareta de hensyn som også flertallsforslaget søker å ivareta. Det vises til *Scheas* begrunnelse og til Riksadvokatens innspill til Metodekontrollutvalget, omtalt i utredningen på side 311.

Forøvrig har NAST følgende merknader:

b) Sentrale tema

Det er bred enighet om at det er "sakens dokumenter" som er gjenstand for innsyn. Det er ingen uenighet om at tiltalte skal ha innsyn i sakens dokumenter, med mindre et dokument er særskilt unntatt. Innsynsomfanget avgjøres følgelig av hva som defineres som sakens dokumenter og hvilke konkrete hjemler for unntak som gis.

c) Kravet til relevans – betydningen av påtalemyndighetens skjønn

NAST vil innledningsvis påpeke at man neppe kan regulere seg bort fra at informasjonen som er tilgjengelig i en straffesak til en viss grad må bero på påtalemyndighetens skjønn. Man kan ikke legge til grunn at en regel om at *alle* dokumenter som kommer inn til politiet er å anse som "sakens dokumenter" og er gjenstand for fullt innsyn, vil avskjære påtalemyndighetens vurderinger av hvilke opplysninger som i det hele tatt kommer inn i saken. Det synes derfor noe uklart hva som kan oppnås ved den endring som utvalget foreslår.

En regel om at hver minste flik av informasjon som kommer inn til politiet *helt uavhengig av relevans* blir saksdokument, er uansett ikke egnet til å sikre lik tilgang til informasjon for mistenkte og politiet. Det kan også resultere i en mer tungrodd prosess og vidløftiggjøring av sakene.

NAST mener det må være rom for at politi og påtalemyndighet unnlater å dokumentere opplysninger som *åpenbart mangler relevans* for saken. Rent praktisk vil dette uansett måtte bli løsningen, jf. bemerkningene i det følgende.

De etterforskende myndigheter bruker nødvendigvis skjønn ved informasjonsinnhentingen. Når det eksempelvis foretas en ransaking, skal det gjøres en fortløpende konkret relevansvurdering på stedet av hvilke dokumenter eller gjenstander som faktisk beslaglegges og blir "sakens dokumenter"[1]. Det bør ikke være for store prosessuelle forskjeller på om en relevansvurdering foretas under ransakingen eller ved en senere gjennomgang av beslaget. På samme måte som man har tiltro til at politiet er objektive ved valget av hvilke vitner man avhører, hvilke spørsmål som stilles under avhør, hvilke telefoner det innhentes trafikkdata på eller hvor man leter etter fingeravtrykk og andre tekniske spor, må man ha tiltro til relevansvurderingen under informasjonsinnhentingen. Det er en *grunnforutsetning for vårt prosessystem* at alle aktører har tillit til at politi og påtalemyndighet etter beste evne ivaretar sin absolutte objektivitetsplikt.

Dersom utvalget ikke er komfortable med at informasjonstilgangen i en sak avhenger av konkret skjønnsutøvelse fra påtalemyndighetens side er det selve prosessordningen og ikke innsynsreglene man må se på. Det er ikke ukjent fra særlig kontinental rett at det er domstolene som styrer

---

[1] Jf. Rt. 1986 s. 1149:
"... det vil ikke være hjemmel for å ta med deler av samlingen som etter den undersøkelse som praktisk kan gjøres på stedet, ikke er av betydning som bevis. Det blir en paradoksal situasjon hvis en vurdering politimannen er pliktig til å gjøre ved ransaking ikke tillates gjort av politi eller påtalemyndighet ved gjennomgang av beslaget. Hvor er skjæringspunktet mellom når relevansvurderingen er en plikt og når det blir forbudt?

etterforskingen, og dermed informasjonstilbudet gjennom såkalte etterforskingsdommere. I Norge ligger denne oppgaven hos påtalemyndigheten.

Tiltalte og forsvarer har begrensede muligheter til å påvirke hva som hentes inn ved mange konkrete etterforskingsskritt. Denne forskjellen i informasjonstilgang kompenseres imidlertid ved at enhver tvil om faktum alltid kommer tiltalte til gunst.

I all større etterforsking er det mye informasjon som ikke legges inn i saken, e-poster til kollegaer, innskytelser, hypoteser som sjekkes ut, forundersøkelser før etterforskingsskritt m.v. Forslag som innebærer at enhver faks, e-post eller vurdering som kommer politiet til kjennskap under etterforskingen ukritisk skal formaliseres som et saksdokument, er mer egnet til å drukne saken med trivialiteter enn til å sikre tiltaltes rettssikkerhet. Regelen er som nevnt uansett ikke egnet til å gi tiltalte samme informasjonskontroll som politiet.

De fleste straffesakene NAST arbeider med er svært omfattende, det er et trekk som også har kjennetegnet de fleste saker hvor innsynspørsmålet er kommet på spissen. I en typisk sak vil dokumentmengden i dag (hvor det foretas en relevansvurdering av hva som legges inn) regelmessig være mellom 5.000 og 10.000 sider, noen ganger atskillig mer. Det er ikke gitt at tiltaltes rettssikkerhet styrkes av at informasjonsmengden økes ytterligere utelukkende med dokumenter politiet mener er helt uten relevans for saken.

En har merket seg at utvalget legger til grunn at "påtalemyndigheten ikke lenger vil ha noen skjønnsmessig adgang til å holde opplysninger innhentet i saken utenfor sakens dokumenter" (s. 302 spalte 2); videre at dette er anbefalt også fra EMD-praksis og at "muligheten til å holde opplysninger utenfor innsyn skal reguleres uttømmende i loven".

På side 303 første spalte, mener utvalget at:

> "Andre hendelser som finner sted og undersøkelser politiet foretar i en straffesak bør imidlertid være ettersporbare i sakens dokumenter, for eksempel der det ved konferanser eller telefonsamtaler kommer frem opplysninger eller anførsler *av betydning for saken*" (vår uthevelse).

Det kan synes som om utvalget på tross av sine uttalelser på side 302, ønsker å opprettholde en skjønnsvurdering for hva som skal bli sakens dokumenter. Slik NAST ser det flytter man ved dette bare skjønnsutøvelsen fra spørsmålet om et utarbeidet dokument skal tilhøre sakens dokumenter, til om et slikt dokument skal utferdiges.

Videre anfører utvalget at

> "...begjæringer [...] om innsyn i materiale som politiet i utgangspunktet ikke anser som saksdokumenter i den enkelte straffesak likevel bør imøtekommes så langt andre hensyn ikke taler mot det..." (s. 303 spalte 2).

Dette medfører ytterligere en skjønnsutøvelse av om innsyn skal gis og etter sin ordlyd også en begrunnelsesplikt.

Det kan ikke være tvilsomt at opplysninger av betydning for saken *alltid* er sakens dokumenter, spørsmålet er *hvem* som skal avgjøre om noe har betyding for saken. Dette er en utpreget skjønnsmessig vurdering som det ligger i påtalemyndighetens prosessuelle rolle å foreta.

Opplysninger som *andre hensyn ikke taler mot* å gi innsyn i, vil alltid kunne gis ut. Det hensynet som implisitt alltid ligger til grunn for ikke å gi innsyn, er de *praktiske og kapasitetsmessige* utfordringene det medfører å samle inn og mangfoldiggjøre opplysninger man i utgangspunktet ikke har redigert for straffesak. Hvis dette skal begrunnes konkret hver gang vil det gjennomgående kreve redigering, bearbeiding og innsamling, slik at begrunnelsen faller bort i det den begrunnes. Eventuelt må det klargjøres at ressurs og kapasitetshensyn er adekvate hensyn i avveiningen av om innsyn skal gis.

NAST foreslår at det presiseres i forarbeidene at opplysninger som *påtalemyndigheten finner at åpenbart ikke har relevans* for saken *ikke* faller inn under begrepet "sakens dokumenter".
Som det fremgår kommer man ikke utenom at påtalemyndigheten må sile dokumenter etter relevans, dette følger av gjeldende rett og av utvalgets forslag. Det bør tas inn i lovteksten eller i det minste i forarbeidene.

d) Unntak for politiets interne saksbehandling

Det foreslås innført ett nytt tredje ledd i strpl. § 242. I forslagets første punktum heter det

> "Retten til innsyn omfatter ikke dokumenter utarbeidet som ledd i politiets og påtalemyndighetenes interne saksforberedelse."

Dette er et forslag embetet slutter seg til.

Utvalget foreslår imidlertid et unntak fra unntaket i strpl. § 242 nytt tredje ledd andre punktum;

> "Mistenkte har uansett rett til å gjøre seg kjent med de deler av interne dokumenter som inneholder faktiske opplysninger eller sammendrag eller annen bearbeidelse av faktum som ikke finnes i andre dokumenter mistenkte har tilgang til og som kan antas å ha betydning for saken."

Faktiske opplysninger som ikke finnes i andre dokumenter og som kan antas å ha betydning for saken, er uansett sakens dokumenter. Det følger av hovedregelen om dokumentinnsyn og definisjonen av sakens dokumenter, jf. strpl. § 242, første ledd. En er usikker på om det er behov for en ytterligere presisering av dette.

Videre vil en sterkt advare mot at politiet og påtalemyndighets egne sammendrag og bearbeidelser skal være gjenstand for innsyn. Det er ikke lett å se for seg interne dokumenter av noe verdi for påtalemaktens indre prosesser som ikke inneholder sammendrag, systematisering eller bearbeidelse av faktum. Eksempler på dette vil være avhørsdisposisjoner, arbeidsnotater, innstillinger, prosedyremanuskript og lignende. Det er helt vanlig for aktorer å utarbeide egne systematiseringer av sakens faktum til bruk under hovedforhandling, til dette er det vanlig å få bistand av etterforsker, det er uheldig hvis dette skal måtte gis til forsvarer som et saksdokument.

Dette er typisk interne notater som er skrevet i en form som ikke er beregnet på innsyn. Hvis det skal gis innsyn må de få en helt annen kvalitetskontroll og formalisering, noe som vil medføre en økt ressursbruk i saksforberedelsesfasen. Videre er forberedelse i aktorteamet noe som pågår gjennom hele saken. Flere ved embetet har for eksempel erfaring med at en ser viktige sammenhenger i trafikkdata dagen før prosedyre når de siste forberedelser gjøres. Skal slike

sammenhenger da gis innsyn i på forhånd, med frist, utsettelse osv? Forslaget innebærer etter NASTs mening en utidig innblanding i aktors saksforberedelse og vil skape kunstige vegger i aktorteamet, særlig i større saker. Hvis forsvarer vil ha ytterligere faktasammendrag gis det hjemmel til å be om det i strpl. § 265.

NAST anerkjenner imidlertid tiltalte og hans forsvarers legitime behov for å få oversendt store informasjonsmengder i håndterlig og systematisk format. Eksempelvis vil det etter embetets syn ikke være tilstrekkelig at forsvarer får trafikkdata i råtekst, mens politiet sitter på søkbare Excelfiler. Det samme vil typisk gjelde transaksjonsoversikter i store økonomisaker etc. Etter embetets syn følger imidlertid en slik praksis allerede av god påtaleskikk. Det vises videre til at utvalget foreslår et tillegg til strpl. § 264 første ledd, som lyder:

> "...og sørger for at sakens dokumenter og andre bevis blir gjort tilgjengelig for forsvareren på forsvarlig og hensiktsmessig måte."

Dette kravet vil etter vårt syn ivareta forsvarerens krav om rimelige arbeidsforhold og hensiktsmessig organisering av materialet som overleveres.

NAST foreslår at utvalgets forslag til ny strpl. § 242, tredje ledd, annet punktum strykes.

e) Innsyn i andre saker

Utvalget foreslår et vurderingstema for når opplysninger fra andre saker tas inn i "sakens dokumenter". Vurderingstemaet inntas i forslag til nytt sjette ledd i strpl. § 242:

> "Mistenkte har rett til å gjøre seg kjent med dokumenter fra andre saker i den utstrekning de kan antas å ha betydning for saken"

Vilkåret "betydning for saken" skal tolkes som en lavere terskel for innsyn enn betydning for skyld eller straffespørsmålet. Terskelen må tolkes i lys av Høyesteretts uttalelser i Rt. 2007 s. 1435 avsnitt 38 – 41, hvor det fremkommer;

> "Ved vurderingen [...] må påtalemyndigheten ha for øye hvordan opplysningene vil kunne brukes fra en forsvarers ståsted."

Med den lave terskelen for innsyn i andre saker som foreslås og med det perspektivet som skal legges til grunn også for rettens vurdering, frykter NAST flere uheldige konsekvenser. Politi og påtalemyndighetens muligheter til å skjule sensitiv informasjon blir for liten og for usikker. En får nå en situasjon hvor saker med sensitiv informasjon ikke slutter å være brennbare selv etter at de er rettskraftig avgjort. Det har videre uheldige konsekvenser for personvernet at eksempelvis kommunikasjonskontrollsamtaler fra henlagte saker lett kan bli saksdokumenter i andre saker. En risikerer også en uheldig vidløftiggjøring av straffesakene.

Det er retten som skal ta stilling til om opplysningen har betydning for saken, det er imidlertid en svært vanskelig oppgave for en uavhengig domstol å ta stilling til betydningen av opplysninger i ett stort og ukjent sakskompleks for en tiltalt i et annet stort og ukjent sakskompleks. Tvil om dette skal komme tiltalte til gode, og en skal ta med i vurderingen at tiltalte og hans forsvarer kan sitte på ellers ukjent informasjon som gjør opplysningen relevant. Embetet frykter at innsyn i andre saker raskt blir den egentlige hovedregelen. Innsyn i andre saker er ikke direkte overførbart med utvidet innsyn i egen sak. Andre saker inneholder intime opplysninger om andre personer, deres personvern fordrer at det foretas en grundig og reell avveining av kryssende hensyn før saksdokumentene spres til uvedkommende. At det skal være høy terskel for innsyn i en straffesak fremgår eksempelvis av påtaleinstruksen § 4-2, 3. ledd.

NAST foreslår at terskelen for innsyn i andre saker settes betydelig høyere enn utvalgets utkast legger opp til. Konkret foreslås det å speile vilkåret i strpl. § 242a, tredje ledd, slik at ny lovtekst i strpl. § 242 sjette ledd eksempelvis kunne utformes slik;

> "Mistenkte har ikke rett til å gjøre seg kjent med dokumenter fra andre saker med mindre manglende innsyn vil medføre vesentlige betenkeligheter av hensyn til mistenktes forsvar."

Forslaget vil harmonisere regelverket når innsyn er henholdsvis utgangspunkt og unntak. Det bør opereres med samme terskel og avveining for å ta inn en opplysning som ikke hører til saken som å ta ut en opplysning som hører til saken. Forslaget vil innebære at det kun åpnes for innsyn i opplysninger fra andre saker når innsyn har betydning for dommens innhold til tiltaltes gunst.

f) Skjæringspunktet for dokumentinnsyn, vern av inngangsopplysninger

Tilslutning til *Scheas* særvotum

NAST slutter seg til argumentasjonen og forslaget fra utvalgsmedlem *Schea* gjengitt i Metodekontrollutvalgets innstilling punkt 26.7.11. Etter vårt syn er dette forslaget best egnet til å ivareta behovet for å verne informanter og annen sensitiv inngangsinformasjon. Til *Scheas* forslag bør det presiseres at *"Ikke medfører vesentlige betenkeligheter av hensyn til den siktedes forsvar"* skal tolkes på samme måte som §242a og forslaget fra NAST om vilkår for innsyn i andre saker. Slik blir reglene om innsyn symmetriske og man får en større base med rettspraksis å trekke den nærmere grense etter.

Ad kapittel 27 - Anonym vitneførsel

NAST viser her til uttalelsen fra Kripos. Som Kripos har også embetet eksklusiv kompetanse når det gjelder krigsforbrytersaker, forbrytelser mot menneskeheten og folkemord. I disse sakene kan det oppstå spørsmål om anonym vitneførsel, noe som er vanlig i sakene behandlet i de internasjonale tribunaler, og embetet foreslår derfor som Kripos at det inntas i straffeprosessloven henvisning til de aktuelle bestemmelsene.

Med hilsen

Siri S. Frigaard
førstestatsadvokat

Inger Marie Sunde
førstestatsadvokat