



Politiets Fellesforbund

Postadresse: Holmenveien 39, 0179 Oslo Tlf: 22 16 31 00

Besøksadresse: Møllergata 30, 4 etg. Faks: 22 16 31 40

E-post: pf@pf.no

Internett: www.pf.no

Org. nr.: NO 871 090 757

Bankkonto: 1600 42 56700

Justis- og politidepartementet
Postboks 8005, Dep

0030 OSLO

Vår dato: 01.05.2010

Vår ref.:

Saksbehandler: ACG

Deres dato:

Deres ref.:

Høring – Metodekontrollutvalget – NOU 2009:15.

Samfunnets behov for beskyttelse har økt i takt med kriminalitetsutviklingen, også sett i lys av den teknologiske utviklingen. Norge må i likhet med resten av verden være forberedt på ytterligere økning i kriminaliteten i årene som kommer, både når det gjelder omfang og alvorlighetsgrad.

Politiet har de senere årene blitt tildelt en rekke nye "verktøy" (les: metoder) som skal sette oss i stand til å bekjempe organisert og annen alvorlig kriminalitet på en god måte. Kriminalitetsbildet med et stort og økende innslag av internasjonal, organisert kriminalitet har aktualisert dette. Metodekontrollutvalget ble gitt et mandat som omfattet en evaluering av nye etterforskningsmetoder og skjulte tvangsmidler som ble innført i 1999 samt påfølgende endringer i 2005. Utvalgets utredning er viktig og svært omfattende. Politiet Fellesforbund (PF) har valgt å kommentere følgende områder:

1. Kommunikasjonskontroll

Kommunikasjonskontroll etter straffeprosessloven kap. 16 innbefatter politiets adgang til å avlytte samtaler eller annen kommunikasjon til og fra bestemte telefoner, datamaskiner eller annen elektronisk kommunikasjon. Det er retten som er kompetent myndighet og som gir politiet tillatelse etter begjæring, likevel slik at påtalemyndigheten på vilkår er gitt en hastekompetanse med retten som etterkontrollør.

Det er foretatt en gjennomgang av hvilke kriminalitetstyper og konkrete straffebud som bør omfattes av straffeprosesslovens § 216a. PF har følgende kommentarer til utvalgets innstillinger:

1.1 Menneskesmugling

PF ønsker å uttrykke tilfredshet med utvalgets innstilling om at utlendingslovens § 47, som omfatter menneskesmugling bør tilføyes og omfattes av § 216a. Organisert menneskesmugling øker i takt med stadig økende forskjeller mellom den rike og den fattige delen av verden. Norge vil således fremstå som et attraktivt land for kriminelle aktører, - som hover inn store penger på menneskeskjebner som utnyttes på det groveste.

Utvalget poengterer at de smuglede er svært sårbare personer som ikke vil kunne være gjenstand for tvangsmiddelbruk. PF er på prinsipielt grunnlag enig i dette, men ønsker å understreke ofte vil bakmenn som smugler barn til Norge utstyre ofrene med telefoner og benytte disse til å gi ordre (jf. Kineserbarnsaken).

Det bør derfor være mulig å avlytte telefoner som reelt sett eies av bakmenn, men som disponeres av ofrene. Erfaring har vist at disse bakmennene ofte oppholder seg i land hvor det er juridisk/praktisk krevende å få iversatt kommunikasjonskontroll.

1.2 Menneskehandel

Ofre for menneskehandel er ofte ikke villige til å samarbeide med politiet. Dette kan ha sin forklaring i grove trusler fra bakmenn, psykisk manipulering eller liten tillit generelt etter dårlig erfaring med politiet i hjemlandet. Etterforskning av slike saker er svært vanskelig blant annet på bakgrunn av disse forholdene.

Det er i dag ikke åpnet for å foreta kommunikasjonskontroll i saker som omfatter simpel menneskehandel. PF ønsker å anføre at dette vil være et viktig virkemiddel for å bekjempe menneskehandel.

Det vil ofte være vanskelig på et tidlig stadium å avdekke hvor alvorlig slike saker er. Erfaringer viser at det vil være av stor betydning for resultatet å få avdekket bakmenn, nettverk, arbeidsmetode og virksomhet, tidligst mulig i etterforskningsfasen. Vi mener derfor at muligheter for kommunikasjonskontroll også bør omfatte simpel menneskehandel. Slike metoder vil være avgjørende for å komme videre i etterforskningen, nettopp fordi man mangler gode, alternative etterforskningsmetoder.

PF mener at hallikvirksomhet også bør omfattes og gi grunnlag for kommunikasjonskontroll. Her vil vi vise til regjeringens handlingsplan mot menneskehandel for 2006-2009, hvor det fremkommer at man vurderer endringer i lovverket for å gi politiet adgang til å benytte særskilte etterforskningsmetoder, også i disse sakene.

1.3 Grooming – internettrelaterte seksuelle overgrep

Straffeloven § 201 a gjør det straffbart å forberede et møte med et barn, hvor forsettet er å begå en seksuell handling (grooming). Straffebudet kom som en konsekvens av den teknologiske utviklingen, hvor bl.a internett har gitt overgripere nye arenaer og treffpunkter for å møte potensielle ofre (barn). Forsøk på "grooming" medfører også straffeansvar.

Bestemmelsen ble innført for å gi barn et bedre vern mot seksuelle overgrep, men også med en intensjon om å klargjøre når politiet kunne iverksette tvangsmidler i forebyggende øyemed, eller etterforskning av slike saker.

PF er opptatt av å sikre barns rettssikkerhet. Vi mener at kommunikasjonskontroll eller andre utradisjonelle metoder er nødvendig for å kunne beskytte barn mot overgrep på en effektiv og tilfredsstillende måte. Vi ønsker i denne sammenheng å påpeke at ingen til nå er domfelt for "grooming" i Norge. Dette er et svært vanskelig område å etterforske. Manglende fellende dommer gjenspeiler ikke mangel på aktuelle saker eller aktuelle overgripere. Det mangler heller ikke fokus eller prioritering fra politiets side. Vi mener at manglende fellende dommer i rettsystemet, viser et reelt behov for utradisjonelle etterforskningsmetoder (kommunikasjonskontroll) for å kunne avdekke og etterforske slik saker.

I tillegg mener vi at kommunikasjonskontroll bør kunne knyttes til straffeloven § 204a. Internett skal ikke være et friområde for pedofile nettverk som distribuerer filmer og bilder som viser grove seksuelle overgrep mot barn. Vi vil understreke at etterforskning av slike saker ofte vil kunne avdekke reelle overgrep. PF mener politiet må tildeles verktøy i takt med den teknologiske utviklingen for å kunne bekjempe de kriminelle effektivt på de arenaene de befinner seg, - i dette tilfellet i den digitale verden.

1.4 Forbund om ran

Politiet har de senere årene hatt relativt god kontroll på ransmiljøet i Norge. Samfunnet har derfor vært forskånet for større ran eller ransforsøk etter Nokas, hvor mange aktuelle aktører innen dette kriminelle miljøet i ettertid måtte sone lengre dommer. Vi skal imidlertid ikke gå lenger enn til Sverige for å se at internasjonale, kriminelle nettverk har stått bak større ran av pengeinstitusjoner og verditransporter. Det vil være naivt å tro at vi vil være forskånet for dette også i fremtiden.

Erfaring viser slike ran er svært godt planlagt og utføres på en veldig profesjonell måte. Straffeloven § 269 hjemler at den som inngår forbund om ran straffes med fengsel inntil tre år. Den lave strafferammen gjør imidlertid at det ikke er adgang til å bruke kommunikasjonskontroll – selv ikke i tilfelle hvor forbundet skjer som ledd i en organisert kriminell virksomhet.

PF mener derfor at politiet bør ha muligheter til å benytte kommunikasjonskontroll også i saker som omfatter "forbund om ran". Dette kan løses på to måter; enten ved å øke strafferammen i strl. § 269 til 5 år, eller ved å innta § 269 i sentrale bestemmelser som hjemler metodebruk (eks. strpl. §216a).

Brutaliteten og profesjonaliteten i ranene som har vært gjennomført de senere årene, har vist at dette er nødvendig for å kunne bekjempe disse miljøene på en effektiv måte. PF ønsker å poengtere at hovedintensjonen med en slik utvidelse er å kunne avdekke planer om ran og deretter forhindre at disse blir gjennomført.

1.5 Kommunikasjonskontroll knyttet til person

I saker som omfatter organisert kriminalitet er det kjent at de involverte kriminelle aktørene svært ofte bytter simkort og/eller telefoner for å unngå at politiet identifiserer hvilke telefoner eller telefonnummer de benytter. I tillegg til taktiske utfordringer er dette også en ressursmessig utfordring for politiet, da ny begjæring om kommunikasjonskontroll må fremmes for retten hver gang et nytt telefonnummer tilknyttet mistenkte blir identifisert.

PF mener derfor at man bør kunne knytte en tillatelse til kommunikasjonskontroll til mistenkte som person, og ikke til en konkret telefon eller telefonnummer som mistenkte disponerer. På denne måten vil de formelle prosedyrene forenkles. Dette vil være ressursbesparende for både politi og rettsvesen. For å ivareta rettssikkerheten kan man i likhet med dansk rett, innføre en rapporteringsplikt for politiet overfor retten, - når nye telefonnummer tilknyttet en bestemt person blir identifisert og avlyttet.

2. Skjult fjernsynsovervåkning

Utvalget har kommet frem til en anbefaling der man bør tillate skjult fjernsynsovervåkning på privat sted, dersom dette begrenses til fellesarealer som trappeoppgang, loft og kjeller eksempelvis tilknyttet et borettslag. Rettspraksis har til nå gitt tillatelse til skjult fjernsynsovervåkning (etter straffeprosessloven § 202a) fra offentlig sted mot et inngangsparti som vil kunne karakteriseres som et privat sted. Dette er begrunnet med at politiet i etterforskningsøyemed har hatt et behov for å kunne kartlegge hvem som frekventerer et hus eller en leilighet.

Utvalget ønsker imidlertid ikke å tillate skjult fjernsynsovervåkning i rom som bebos. PF mener at skjult fjernsynsovervåkning også bør tillates på enkelte private steder, nettopp for å kunne gjøre f.eks romavlytting mer effektiv. Til sammen vil disse metodene kunne være en mindre inngripen overfor personene som utsettes for skjulte tvangsmidler, spesielt ettersom man vil få mer presis informasjon på et tidlig tidspunkt i etterforskningen. Vi mener at dette trolig vil begrense tidsperioden for nødvendig metodebruk.

3. Overskuddsinformasjon

Det er i dag ikke anledning til å benytte informasjon som fremkommer under bruk av skjulte tvangsmidler, som bevis i retten i andre saker enn den saken som var bakgrunnen for iverksettelsen av tvangsmiddelet. Utvalget går inn for at denne bestemmelsen skal endres slik at overskuddsinformasjon som fremkommer ved bruk av skjulte tvangsmidler også kan benyttes som bevis for forhold utover det opprinnelige straffbare forholdet.

Et eksempel kan være at politiet i en pågående narkotikaetterforskning får håndfast informasjon via kommunikasjonskontroll at NN har begått et ran. Det vil i en slik situasjon fremstå underlig om NN ikke kan bli domfelt på bakgrunn av bevis som fremkommer i KK materialet.

PF er enig i flertallets syn på dette området og mener at behovet for å oppklare og iretteføre straffbare handlinger tilsier at overskuddsinformasjon må kunne benyttes som bevis i alle typer straffesaker. Dagens situasjon synes i tillegg å stride mot vanlige folks rettsoppfatning.

4. Anonym vitneførsel

Kriminalitetsutviklingen med en stadig større andel av internasjonale, kriminelle aktører har aktualisert behov for å beskytte personer som gir informasjon til politiet. Utenlandske kriminelle miljø som opererer i Norge er kjent for å benytte hard "indrejustis" for å kontrollere involverte personer. Det kan få fatale konsekvenser dersom det fremkommer at noen i miljøet har samarbeidet med politiet.

Politiet er helt avhengig av f.eks bruk av informanter for å kunne bekjempe denne type kriminalitet på en effektiv måte. Det er derfor viktig at man overfor potensielle informanter eller vitner i saker, i spesielle tilfeller, kan garantere full anonymitet. Dette er avgjørende for at viktig informasjon fra ellers svært lukkede miljø skal tilflyte politiet. Tilsvarende gjelder også i saker der norsk politi mottar informasjon fra utlandet.

PF imøteser derfor forslag til endringer i straffeprosessloven som vil åpne for å hemmeligholde informantens identitet i større omfang og på bedre vilkår enn det som er tilfelle i dag.

5. Innhenting av trafikkdata

Politiet Fellesforbund avga for kort tid siden høringssvar som omfattet forslag om implementering av EUs datalagringsdirektiv. Høringssvaret omhandlet i stor grad aktuelle momenter tilknyttet politiets mulighet for innhenting av trafikkdata og vi viser derfor til dette høringssvaret i sin helhet. Høringssvaret vedrørende DLD ligger vedlagt.

6. Prosessuelle fellesspørsmål – muntlige forhandlinger

Utvalget foreslår at det innføres en ordning hvor samtlige begjæringer som fremmes retten angående tillatelse til bruk av skjulte tvangsmidler, som hovedregel skal avholdes ved muntlige forhandlinger. Utvalget mener man ved dette vil bedre forutsetningene retten har til å fatte en reell vurdering av begjæringen, og at oppnevnt advokat vil kunne gis bedre anledning til å fremme innsigelser.

PF mener at dette ikke er en god løsning, men en ordning som vil kunne vanskeliggjøre behandling av hastersaker, der en hurtig "reaksjon" ved bruk av skjulte tvangsmidler vil være avgjørende for resultatet. Vi mener videre at den ressursmessige belastningen både for politi og påtalemyndighet, samt retten - Ikke vil kunne forsvare en slik ordning. Under enhver omstendighet er det viktig at påtalemyndigheten bevarer muligheten til å behandle saker som krever umiddelbar iverksettelse av tvangsmidler.

7. Advokaters taushetsplikt i straffesaker

PF er enig i utvalget sin konklusjon om at det er behov for å lovfeste en generell taushetsplikt for advokater og andre som utfører arbeid for et advokatkontor, knyttet til opplysninger om personlige forhold og bedriftshemmeligheter som de får kjennskap til i straffesaker.

Vi ser det som naturlig at alle aktører i straffesakskjeden pålegges samme taushetsplikt knyttet til slike opplysninger. PF er videre enige i at brudd på taushetsplikten også skal medføre straffeansvar.

8. Kontrollen med politiets bruk av skjulte tvangsmidler

Utvalget berører i kapittel 11 mange ulike instanser og perspektiver som omfatter kontrollen med politiets bruk av skjulte tvangsmidler. PF ønsker å understreke at den beste måten å hindre misbruk og utøve kontroll på, er å utvikle medarbeidernes kompetanse, sikre god ledelse og jobbe målrettet for en organisasjonskultur som er opptatt av åpenhet, erfaringslæring og god etikk.

9. Ressursmessige konsekvenser

PF vil bemerke at utvidede muligheter til metodebruk, medfører større kostnader. Det må hyppig foretas vanskelige prioriteringer. Tildelte budsjett setter store begrensninger for hvor omfattende etterforskningen i de enkelte straffesakene er.

Kriminalitetsutviklingen med stadig større innslag av internasjonale og ofte organiserte, kriminelle nettverk krever økt bruk av utradisjonelle metoder. Tolkeutgifter har økt proporsjonalt med denne utviklingen. Det samme har utgifter som faktureres av teleleverandører i forbindelse med uthenting av trafikkdata og kommunikasjonskontroll.

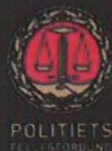
Politidirektoratet har utarbeidet en driftsanalyse for perioden 2002-2008. Denne analysen viser et bilde av ressursutviklingen i perioden. Straffesaksutgifter som fremkommer av analysen ville trolig vært enda større dersom politiet hadde hatt ressurser til å drive mer grundig og omfattende etterforskning.

PF vil derfor påpeke at nye kostnadskrevende (dog nødvendige) metoder, må følges opp slik at driftsbudsjettene ikke skal være avgjørende i forhold til hvor effektive og profesjonelle politiet er i bekjempelsen av kriminalitet. Det er et stort behov for tilførsel av "friske midler".

PF mener videre at det er viktig å ikke bare se på kostnader i et kort perspektiv, men også se hen til den preventive effekten, - når politiet kan fremstå som tydelige, effektive og handlekraftige overfor tunge, organiserte, kriminelle miljøer. Dette er gode investeringer og av stor betydning for både samfunnet og enkeltindivider.


Arne Johannessen
Forbundsleder


Anne-Catherine Gustafson
Forbundssekretær



Politiets Fellesforbund

Postadresse: Møllergata 39, 0179 Oslo

Telefon: 23 16 31 00

E-post: pf@pf.no

Organ nr.: NO 871 001 352

Besøksadresse: Møllergata 39, 4 etg

Faks: 23 16 31 40

Internett: www.pf.no

Bankkonto: 1600 42 38700

Samferdselsdepartementet
Postboks 8010, Dep.

0030 OSLO

Vår dato: 12.04.10

Vår ref.:

Saksbehandler: Anne-Catherine Gustafson

Deres dato:

Deres ref.:

Høring – EUs datalagringsdirektiv

Innledning

Politiet har et oppdrag hvor vi er satt til å bekjempe kriminalitet og skape trygghet i befolkningen. Publikum har store forventninger til løsningen av denne oppgaven. Politikere har i tillegg store forventninger som tydeliggjøres bl.a. gjennom pålegg og prioriteringer. Skal vi klare å innfri disse forventningene må vi være tydelige på hvilke verktøy politiet er avhengige av, for å løse oppgaven på en god og tilfredsstillende måte.

Ett av de mest sentrale spørsmålene som har utkrystallisert seg i debatten rundt datalagringsdirektivet, har vært en avveining mellom samfunnets behov for verktøy i kriminalitetsbekjempelsen opp mot personvern hensyn.

Vi ønsker i det følgende å redegjøre og begrunne PF sitt syn på forslag som foreligger fra regjeringen vedrørende implementering av EUs datalagringsdirektiv i Norge.

Hovedpunkter som vil bli berørt er:

- **Informasjonssikkerhet og personvern**
- **Gjeldene rett og praktisering**
- **Beskrivelse av politiets behov for verktøy – dagens realiteter og fremtidens utfordringer**

1. Informasjonssikkerhet og personvern

Sikkerheten rundt informasjonen som teletilbydere skal håndtere er avgjørende for om personvernet blir ivaretatt på en god måte. Datalagringsdirektivet stiller krav om informasjonssikkerheten hos tilbyderne som i stor grad allerede er ivaretatt gjennom dagens regelverk. Det er kun autorisert personell som også i fremtiden skal ha tilgang til lagrede trafikkdata og ulike tilsynsordninger er foreslått for å tilse at pålegg som omfatter informasjonssikkerhet blir ivaretatt på en lovmessig og god måte.

Straffeprosessloven ivaretar personvernet og rettssikkerheten til den eller de som er mistenkt eller siktet i en straffesak. I tillegg finnes det en rekke lover som regulerer og sanksjonerer urettmessig innsyn.

Et annet aspekt er at informasjonen som i dag lagres er såkalte "rådata" som ikke er lesbare eller analyserbare før man har bearbeidet dette teknisk. Bearbeiding av disse "rådataene" skjer først av politiet når hjemmel for innsyn er til stedet og politiet besitter denne informasjonen. PF mener at dette også er med på å ivareta sikkerheten i forhold til urettmessig Innsyn.

Politiregisterloven som nylig ble vedtatt av Stortinget mener vi i tillegg vil være med på styrke den enkeltes rettsikkerhet og personvern. Samtidig ønsker vi å påpeke at de viktigste tiltaket mot misbruk er åpenhet, kompetanse og god samfunnskontroll.

PF mener at direktivets krav til informasjonssikkerhet samt lover som regulerer politiets tilgang til disse dataene, ivaretar samfunnet og enkeltindividets behov for sikkerhet og personvern. Vi mener i tillegg at **personvernet** vil bli styrket gjennom en implementering av datalagringsdirektivet, nettopp fordi slike opplysninger stadig oftere benyttes i etterforskningen og er avgjørende for å bevise både skyld og uskyld.

Debatten når det gjelder datalagringsdirektivet har ofte vært knyttet til refleksjoner rundt personvernet. PF mener at personverndebatten i alt for liten grad har reflektert over offerets rett til personvern og rettsikkerhet f. eks i overgrepssaker der overgrepsmateriale i ettertid av har blitt spredt over internett. Personvernet og rettsikkerheten er viktig for alle, også for barna som blir utsatt for overgrep. Et nei til direktivet mener vi vil styrke de kriminelle sitt personvern og svekke de svakeste.

Det har i debatten fremkommet påstander om at vi vil få et "overvåkningssamfunn" ved en innføring av datalagringsdirektivet, hvor 4,8 millioner innbyggere kriminaliseres. Denne påstanden mener vi er misvisende. Tradisjonell overvåkning innebærer at et statsorgan aktivt innhenter informasjon om borgerne. Dette er ikke tilfelle ved en implementering av datalagringsdirektivet. I denne saken er man fra politiets side opptatt av at sletting av eksisterende, historiske trafikkdata utsettes. De aller fleste av trafikkdataene som omfattes av direktivet blir allerede lagret i dag, og blir benyttet av politiet ved behov i forebygging, etterforskning og iretteføring av straffesaker.

PF ønsker å påpeke at f. eks ved bruk av trafikkdata i initialfasen av en etterforskning, vil man kunne unngå metodebruk som vil kunne karakteriseres som et større inngripen enn innsyn i hvem mistenkte/siktede har kommunisert med, hvor og på hvilket tidspunkt. En innføring av direktivet menet vi derfor en trygghet både i et rettsikkerhetsperspektiv og av personvernmessige hensyn.

EUs datalagringsdirektiv legger opp til et godt, helhetlig rammeverk for håndtering av denne type informasjon. PF mener at direktivet vil sikre et bedre personvern enn det som er tilfellet i dag, hvor trafikkdata blir lagret utelukkende på grunnlag av teletilbydernes kommersielle behov.

Debatten rundt EUs datalagringsdirektiv har i stor grad til nå vært farget av at enkelte aktører ikke har hatt fokus på hva som dagens situasjon og hva en innføring av datalagringsdirektivet vil medføre av reelle endringer. Pkt 2.2 og 2.3 vil redegjøre for dette.

2. Gjeldene rett og praktisering

Det finnes i dag ingen lovbestemt plikt for teletilbyderne til å lagre trafikkdata. Utgangspunktet for dagens praksis er at teletilbyderne har fått tillatelse til å lagre trafikkdataopplysninger av Datatilsynet, grunnet faktureringshensyn og/ eller i kommunikasjonsformål.

Teletilbyderne er videre ilagt en sletteplikt av disse dataene (Ekomloven §2-7), når formålet med lagringen er borte. I dag er det svært ulik praktisering hos teletilbyderne, noe som f. eks gjør seg gjeldene hva angår lagringstid.

Når det gjelder lagring av telefonidata varierer denne fra 3 til 5 måneder hos hhv Telenor og NetCom. Data knyttet til internettbruk slettes nå etter 3 uker etter pålegg fra Datatilsynet. Dette pålegget endret og minsket politiets mulighet til å etterforske internettrelatert kriminalitet betraktelig.

Justisdepartementet gjorde i 2008 noen betraktninger vedrørende dagens lagringspraksis hos teletilbyderne etter å ha innhentet opplysninger fra disse. Departementet påpeker den ulike praktiseringen og er videre tydelige på at nesten alle tilbyderne av fasttelefoni lagrer data i dag som EU's datalagringsdirektiv krever, og at de fleste tilbyderne av mobiltelefonitjenester gjør det samme.

I forhold til trafikkdata som omfatter bruk av internett oppsummerer de med at de fleste tilbyderne lagrer navn på abonnent som foretar tilkobling og dennes IP adresse, og at halvparten i dag lagrer resterende data som etterspørres av direktivet. Når det gjelder e-post lagrer noen av tilbyderne (under halvparten) de data som etterspørres i direktivet.

PF mener med dette at det i all hovedsak ikke vil foreligge vesentlige endringer ved en eventuell implementering av direktivet sammenliknet med dagens praktisering for lagring av trafikkdata. Dagens praktisering kommer som følge av teletilbydernes behov for lagring av trafikkdata, noe som utelukkende er tuftet på forretningsmessige hensyn (fakturering av kunder).

Etter PF's oppfatning er tiden overmoden for en regulering av praksisen rundt datalagring. Dette må videre sees i et samfunnsmessig perspektiv, hvor behov for trygghet og bekjempelse av alvorlig og organisert kriminalitet bør bli vektlagt.

2.1 Uthenting av trafikkdata

Dersom det foreligger opplysninger om at trafikkdata oppbevares hos tilbyder (eks NetCom/ Telenor), kan politi- og påtalemyndighet be Post og teletilsynet eller retten som kompetent myndighet om å fritta tilbyderne for taushetsplikten. Rettsvesenet kan da beslaglegge elektroniske spor f. eks knyttet til telefoni.

Hver anmodning som Post og teletilsynet mottar vedrørende fritak fra taushetsplikten vurderes på selvstendig grunnlag mot straffeprosessens vilkår.

Tilsynet foretar en konkret avveining mellom hensynet til personlig integritet og personvern, opp mot politiets behov i etterforskning av konkrete straffesaker og samfunnets ønske om bekjempelse av kriminalitet.

Politiet benytter i utstrakt grad i dag informasjon fra teleselskapene for å forebygge kriminalitet eller under etterforskning av straffesaker og senere eventuelt som bevis i retten. Informasjonen benyttes ofte for å dokumentere hvor en eller flere mistenkte/siktede har vært på ulike tidspunkt, avdekke nettverk og f. eks hyppigheten av kommunikasjonen. Elektroniske spor som mistenkte eller siktede har etterlatt seg ved f. eks bruk av mobiltelefon, har blitt benyttet i rettssaker siden tidlig på 1990-tallet. Dette er på ingen måte noe nytt.

Departementet foreslår en endring av dagens lovverk ved at det kun skal være retten som skal kunne pålegge teletilbyder å utlevere tilgjengelig data. PF er bekymret for at man ved en slik praksis vil kunne forsinke etterforskningen av straffesaker betraktelig. Dette ved at en allerede overbelastet instans i tillegg skal måtte behandle rundt 2000 anmodninger i året fra politiet.

PF mener i tillegg at dagens regelverk som innbefatter at utlevering kan foretas i saker hvor trafikkdata "antas å ha betydning som bevis" (straffeprosesslovens Kap 16) bør opprettholdes. En innskjerpelse av mulighetene til å innhente trafikkdata f. eks i saker hvor en mistanke ikke knytter seg til en bestemt person, vil være et paradoks sett i relasjon til direktivets intensjon, nemlig å bekjempe alvorlig kriminalitet.

3. Beskrivelse av politiets behov for verktøy – dagens realiteter fremtidens utfordringer?

3.1 Kriminalitetsutviklingen

Kriminalitetsutviklingen viser en stadig økende andel av organiserte, profesjonelle, utenlandske aktører som kommer til Norge utelukkende for å begå kriminalitet. Det stilles krav til politiet fra samfunnet side at vi møter disse utfordringene med profesjonalitet og effektive verktøy. Trafikkdata er et svært viktig verktøy for politiet, men det vil være uholdbart i lengden at tilgangen til slike data er mer eller mindre tilfeldig og uforutsigbar slik det fremstår i dag.

Den teknologiske utviklingen gjør at en stadig større andel av kommunikasjonen skjer elektronisk (f. eks virtuelle arenaer). De kriminelle er i likhet med befolkningen for øvrig på disse arenaene. PF mener at dagens lovverk er i uttakt med kriminalitetsutviklingen og at en opprettholdelse av dagens regelverk er en trussel mot rettssikkerheten.

For politi og samfunnet er bruken av trafikkdata et av våre viktigste verktøy i bekjempelsen av organisert og annen alvorlig kriminalitet. Bruk av elektroniske spor har eskalert i takt med den teknologiske utviklingen og kriminalitetsutviklingen. Dette blir benyttet innen en rekke ulike sakstyper som organisert vinningskriminalitet, drap, vold og sedelighet, økonomisk kriminalitet, narkotika, menneskehandel og saker som omfatter forebygging av terrorvirksomhet.

3.2 Betydning av elektroniske spor?

Elektroniske spor omtales ofte som såkalte "tause vitner" og har fått en stadig større betydning for politiets arbeid spesielt relatert til bekjempelse av organisert og annen alvorlig kriminalitet. Utviklingen av arbeidsmetoder som benyttes i tunge, kriminelle miljø (MC/narkotika/menneskehandel), viser at vitner trues til taushet og gjør viktigheten av elektroniske spor desto større. Ordene "tause vitner" får derved en videre betydning.

For å gi et bilde av hvor avgjørende trafikkdata er i etterforskningen av ulike straffesaker redegjøres det i det følgende for noen sakstyper hvor trafikkdata er og har vært helt essensielt:

Mobile vinningskriminelle – seriesaker

OP Grenseløs i Vestfold har siden vinteren 2007 etterforsket og iretteført en rekke saker som omfatter organiserte vinningskriminelle nettverk, hovedsakelig fra Øst-Europa. I samtlige av sakene har trafikkdata vært av helt avgjørende betydning. Basestasjonssøk fra åsteder (søk etter hvilke telefonnummer som har vært i nærheten av gjerningsstedet på aktuelt tidspunkt) har bl.a. medført at man har kunnet knytte omfattende seriesaker sammen, som har funnet sted i flere politidistrikt.

I den personrettede etterforskningen har trafikkdata innhentet fra mistenkte/siktede vært av avgjørende betydning for å kunne avdekke oppholdssted, reisevirksomhet, kriminell virksomhet og nettverkstilhørighet.

Drap, vold og sedelighet

I voldssaker blir det om mulig innhentet trafikkdata fra både mistenkt, siktet og fornærmede dersom dette ansees å ha relevans for saken. Er gjerningspersonen ukjent blir det innhentet basestasjonssøk for å forsøke i sirkle inn aktuell person. Trafikkdata er også her viktig for å kontrollere forklaringer som blir gitt, eventuelle aktuelle knytninger mellom fornærmede og gjerningsperson, nettverk, bevegelser og eventuelle ytterligere impliserte.

En overfallsvoldtekt som fant sted i Stavanger 2009 kan illustrere dette:

Høsten 2009 ble en jente på tur hjem fra byen overfalt av 2 personer og voldtatt i en park i Stavanger. I forbindelse med voldtekten forsvant fornærmedes telefon. Trafikkdata på telefonen like etter voldtekten viste ingen aktivitet. Noen dager før jul 2009 ble det foretatt et IMEI-søk på fornærmedes telefon. Søket viste at nytt sim-kort var satt inn i telefonen. Med bakgrunn i dette ble en person pågrepet. Avhør av denne ledet politiet til 2 andre personer som ble pågrepet og varetaktsfengslet. Den ene av disse tilstod voldtekten i fengslingsmøtet.

Narkotikasaker

Alvorlig, organisert narkotikavirksomhet går under benevnelsen "skjult kriminalitet" og som karakteriseres ved at det er få vitner og derfor vanskelige å avdekke, etterforske og irettføre. Kommunikasjonskontroll og andre utradisjonelle etterforskningsmetoder (eks. hemmelig ransaking, romavlytting) blir bl.a. benyttet for å kunne avdekke virksomheten.

Trafikkdata blir i tillegg til å identifisere gjerningspersoner og nettverk benyttet i utstrakt grad for å avdekke hvilke telefonnummer som bør avlyttes for deretter å kunne identifisere og pågripe bakmenn for virksomheten. Saker som dette har ofte internasjonale dimensjoner hvor trafikkdata er helt avgjørende for en god, samordnet etterforskning. Det internasjonale aspektet samt sakenes kompleksitet og omfang, gjør arbeidet svært ressurskrevende.

Internettrelaterte seksuelle overgrep

Den teknologiske utviklingen og internett har skapt en ny arena for seksuelle overgrep. Identifisering av IP-adresser tilhørende overgripere eller personer som deler filer med f. eks barnepornografisk innhold, er helt avgjørende for at man skal kunne straffeforfølge gjerningspersonene. Ovennevnte saker har ofte internasjonale forgreninger, hvor filer med barnepornografisk innhold spres til store deler av verden på kort tid.

Utfordringen i dag er at tilbyderne av internettjenester i Norge er pålagt å slette data etter 3 uker. Dette medfører svært begrensede muligheter for norsk politi til å kunne avdekke overgripere og personer som deler overgrepsmateriale over internett. Problemet er at informasjonen som kan være med å identifisere gjerningspersoner er slettet, og at man derfor i praksis ikke klarer å etterforske og irettføre ovennevnte saker. I tillegg til at personvernet for den enkelte som blir utsatt for overgrep er fraværende, mener PF at det internasjonale politisamarbeidet gjennom et rigid regelverk blir satt på prøve. Det er svært uheldig at utenlandske kollegaer gjentatte ganger opplever at god informasjon ikke blir gjort noe med av norsk politi og ikke genererer resultater eller informasjon tilbake. I tillegg oppfyller vi ikke våre internasjonale forpliktelser som vi har blant annet gjennom FNs barnekonvensjon.

Datakriminalitet

Teknologien åpner som tidligere nevnt kontinuerlig for nye muligheter og arenaer for de kriminelle. Kriminalitetsutviklingen på dette området omfatter bl.a. datainnbrudd, nettbank- og kredittkortbedrageri, id-tyveri samt trakassering og trusler over internett. Ulikt andre straffesaker finnes det her ingen andre alternative etterforskningsmetoder eller spor da kriminaliteten foregår "i den elektroniske verden". Sporene vil nesten alltid innbefatte en IP-adresse, men også her er utfordringen at lagringstiden er så kort at det setter store begrensninger for etterforskningen av disse sakene. Sakene har også her svært ofte internasjonale dimensjoner. Utveksling av informasjon og samordning av etterforskningen i et internasjonalt politisamarbeid er ressurskrevende og ikke minst tidkrevende. Et rigid regelverk med pålagt sletting av data etter 3 uker gir også her store utfordringer når det gjelder å løse oppgaven vi er satt til med å bekjempe kriminalitet av denne typen.

PF mener at en harmonisering av lagringstiden på samtlige av områdene som omfatter trafikkdata er et riktig og viktig virkemiddel. Se punkt nedenfor vedrørende lagringstid og utfordringer med dagens lagringspraksis.

3.3 Lagringstid – utfordringer med dagens praksis

Det er opp til hvert enkelt land å fastslå en lagringstid innenfor direktivets rammer på mellom seks måneder til to år. De fleste land som har implementert EU's datalagringsdirektiv har lagt seg på ett års lagringstid av trafikkdata, så også Danmark og Finland.

PF mener at politifaglige vurderinger og erfaringer bør vektlegges om vi skal kunne bekjempe organisert og annen alvorlig kriminalitet på en god og effektiv måte. Politiets erfaringer tilsier at dagens praksis med kun få måneders lagring (tre og fem mnd.) ikke er tilstrekkelig for å kunne belyse omfanget og alle relevante sider av aktuelle straffesaker.

Det er ovenfor redegjort for hvilke utfordringer dagens regelverk gir, med hensyn til internettrelatert kriminalitet, hvor man har pålagt sletting av data etter tre uker. I andre typer saker har vi følgende å tilføre:

Østfold politidistrikt har med sin beliggenhet nær grensen bl.a store utfordringer når det gjelder grov narkotikakriminalitet. I flere saker blir kurerer pågrepet med store mengder narkotika hvor det fremkommer opplysninger som tilsier at vedkommende har vært på flere og hyppige kurerter det siste året.

Opplysningene er imidlertid vanskelig å verifisere da trafikkdata som kunne ha vært til hjelp i saken er slettet. Tre måneders lagringstid er for kort for å få innblikk i sakens omfang og aktuelle involverte. Lagringstiden begrenser etterforskningene og dermed også sakenes reelle omfang.

Når det gjelder alvorlige overgrep anmeldes dette ofte av fornærmede etter lang tid. Trafikkdata som kan verifisere opplysninger i saken er derfor også oftest slettet og verdifull informasjon er gått tapt. Lengre lagringstid på trafikkdata vil være et viktig verktøy for å etterforske samt irettføre slike overgrep i større grad enn i dag. Et bedre og bredere grunnlag for en eventuell domfellelse vil også da være til stede.

I saker som omfatter menneskehandel kan offeret innvilges seks måneders refleksjonsperiode, hvor man skal benytte tiden til å avgjøre om man ønsker å anmelde forholdet. Dersom offeret etter fem måneder har kommet frem til at man ønsker å anmelde forholdet, er viktige bevis og etterforskningsmateriale som elektroniske spor for lengst slettet med dagens praksis.

PF er enige med departementet som fastslår at man ikke ønsker å skille på lagringstid etter teknologi. PF mener videre at ideelt sett bør man fastslå en lagringstid på to år, og minimum ett år. Dette vil gjøre politiet bedre i stand til å kunne bekjempe organisert og alvorlig kriminalitet på en god og effektiv måte, for samfunnets beste.

3.4 Kostnader

Utgifter til innhenting av trafikkdata har økt kraftig de senere årene. Dette i takt med kriminalitetsutviklingen med stadig større innslag av organisert og annen alvorlig kriminalitet. Det er en kjensgjerning at erfaringsmessig store utgifter knyttet til dette ofte begrenser etterforskningen, fordi disse utgiftene gjør store innhugg i driftsbudsjettene. PF mener det er viktig at Ekomloven endres slik at trafikkdata kan innhentes vederlagsfritt fra teletilbyderne. Vi mener at dette i et samfunnsøkonomisk perspektiv vil være både ressursbesparende og effektivt. Alternativt bør det innføres en sentral refusjonsordning lik den som finnes i dag for sikring av DNA spor og analyser av disse.

3.5 Forslag til innføring av strafferamme

Politiet får i dag utlevert trafikkdata dersom det antas å ha verdi som bevis i straffesaken. I forslaget som foreligger fra regjeringen ligger det en betydelig skjerpelse i forhold til dagens hovedregel, da det foreslås en strafferamme på fengsel i 3 år eller mer. PF ønsker å gi uttrykk for at en slik innskjerpelse vil kunne begrense politiets muligheter til å oppklare alvorlig kriminalitet.

Som eksempel på viktige saker hvor det kan bli vanskelig å få tilgang til trafikkdata dersom foreslåtte strafferamme innføres, er saker der barn og unge blir utsatt for mobbing, trakassering, "grooming", sjikane eller trusler via internett/mobiltelefon. Dette er intet ukjent fenomen i dagens samfunn, og et særdeles viktig område å sette inn ressurser på.

Et annet område som kan nevnes er miljøkriminalitet. Lave strafferammer vil gjøre at sakene blir desto vanskeligere å etterforske dersom man i fremtiden ikke får tilgang til viktig trafikkdata.

I tillegg ønsker vi å trekke frem en sak fra Rogaland som på en god måte kan eksemplifisere at store sakskompleks ofte begynner i det små. Det kan i initialfasen av en etterforskning være vanskelig å se omfanget av sakskomplekset. Noe som i startfasen kan fremstå som et simpelt tyveri, kan vise seg å være organisert kriminalitet.

Tyverier av minibankkort på restauranter med påfølgende uttak i minibank.

Tidlig i juli 2009 ble en rumensk statsborger pågrepet etter tips fra et av utestedene. Han var i besittelse av et stjålet minibankkort som ble knyttet til en av utestedets kunder. Siktete var i besittelse av en mobiltelefon og anropsloggen viste fersk kontakt med to andre mobiltelefoner. Trafikkdata ble innhentet etter samtykke fra Post- & Teletilsynet.

En analyse av innhentet trafikkdata viste at alle tre telefonnumrene i perioden trafikkdata var tilgjengelig, hadde hatt samme "reiserute" mellom Stavanger og Bergen og at personene som disponerte telefonnumrene hadde mye kontakt med hverandre. Det ble opprettet samarbeid med politiet i Haugesund og Bergen for en koordinering av etterforskningen av tilsvarende saker. Trafikkdata var med på å identifisere de to andre personene. Dette medførte at to personer ble pågrepet i Troms politidistrikt.

Trafikkdata på alle tre gjerningspersonene knyttet de til geografisk område over en periode på ca 3 mnd. Dette ble sammenholdt med gjerningssted og gjerningstidspunkt. Etterforskningen endte med tiltale på 122 forhold for tyveri fra person på offentlig sted i Bergen, Haugesund og Stavanger.

Uten trafikkdata har det vært vanskelig å bevise noe annet enn det ene tyveriet førstemann ble pågrepet for.

For øvrig har politiet via andre kanaler identifisert at alle tre personer har vært i Norge i lenger tid enn 3 mnd. Hvis lagring av trafikkdata har vært lenger enn 3 mnd ville politiet trolig hatt mulighet til å oppklare forhold rumenerne kunne mistenkes for, forut for den perioden trafikkdata var tilgjengelig.

PF mener at intensjonen med direktivet kan bli undergravet om en innfører en strafferamme på fengsel i tre år eller mer, jf ovennevnte eksempler. Vi mener videre at ved en eventuell innføring av krav om oppgitt strafferamme, må det nedsettes en arbeidsgruppe som bør se på aktuelle unntak fra bestemmelsen. Unntakene bør omfatte viktig lovbrudd som ikke innehar en strafferamme på 3 år eller mer, og som derved vil kunne ivareta rettssikkerheten.

3.6 Lagringssted

Det er i høringen fremlagt to mulige løsninger for hvor trafikkdata bør lagres. To hovedmodeller er skissert; lagring hos den enkelte tilbyder og lagring i en sentral database. Det finnes i dag et stort antall teletilbydere i Norge, hvor størrelsen på selskapene og antall kunder er svært varierende. PF mener at en sentral database vil være den mest hensiktsmessige løsningen av flere årsaker.

For det første mener vi at den praktiske uthenting av trafikkdata vil bli forenklet ved lagring i en sentral database. Politiets behov for en effektiv og rask håndtering vil derved kunne bli ivaretatt. Dette bl.a ved en standardisering av formatene av trafikkdataene.

For det andre mener vi at lagring i en sentral enhet vil ha store fordeler hva gjelder sikkerhet og kontroll av trafikkdata som foreligger. Erfaringsmessig har vi store utfordringer på dette området i dag med små teleselskaper. Innhenting av trafikkdata vanskeliggjøres da kompetanse og ressurser er manglende. Vi stiller oss tvilende til at små teleselskaper vil kunne ivareta dette på en bedre måte i fremtiden, enn det som er tilfelle i dag. Med en sentral database vil man kunne tilse at både sikkerheten og kontrollen ivaretas, noe som også vil kunne styrke ivaretagelse av personvernet hos den enkelte kunde.

3.7 Politiets tilgang til trafikkdata

Det foreslås en innskjerpelse av dagens praktisering hva angår utlevering av trafikkdata. Dette innebærer forslag om at det kun er retten som skal kunne pålegge besitteren å utlevere data til politiet. PF ønsker å påpeke at dersom denne endringen foretas, hvor det kun er retten som er kompetent myndighet, er det viktig å sikre løsninger som ivaretar muligheter for en rask behandling ved saker som krever iverksettelse av umiddelbare etterforskningskritt.

PF ønsker videre å påpeke at man ved en eventuell innføring av krav om "skjellig grunn" må tilse at dette ikke nødvendigvis må knytte seg til en konkret person. Krav om "skjellig grunn til mistanke" knyttet til en konkret person, vil begrense politiets muligheter til å innhente nødvendig informasjon i viktige saker. I initialfasen av en etterforskning vil det ofte være uklart hvem eller hvilke personer som kan være aktuelle, men en analyse av trafikkdata vil kunne avklare dette tidlig. Det bør imidlertid kunne stilles krav om at innhenting vil være av vesentlig betydning for etterforskningen, lik straffeprosesslovens §202 som omfatter skjult fjernsynsovervåking. Realiseringen av formålet med direktivet vil derved bli ivaretatt.

Avslutning og oppsummering

PF vil fremheve at datalagringsdirektivet møter et behov som i lengre tid har vært til stede, nemlig en lovregulering av hvordan elektroniske spor som trafikkdata skal behandles. Flere har stilt spørsmål ved hvorfor ikke politiet tidligere har vært "på banen" (før diskusjonene rundt datalagringsdirektivet), dersom nevnte metoder har vært så vesentlige som vi fremhever.

Vi ønsker å poengtere at dette temaet har eksistert lenge før debatten rundt datalagringsdirektivet. Dette fremkommer av en rekke høringer bl.a så tidlig som i år 2000 hvor "Sårbarhetsutvalget" nedsatt av Willoch-regjeringen berørte temaet. Videre har Politimetodeutvalget (NOU 2004:6), og Metodekontrollutvalget (NOU 2009:15) hatt drøftinger som omfatter bruk av trafikkdata og behov for en bedre regulering av dagens praksis. Behovet har blitt ytterligere aktualisert fra 2000 og frem til i dag grunnet kriminalitetsutviklingen og den teknologiske utviklingen, samtidig som metodene har blitt utvannet gjennom f. eks datatilsynets pålegg om sletting etter tre uker av visse typer trafikkdata.

Vi mener direktivet i tillegg legger et godt grunnlag for kontroll, og vil gjøre norsk politi og samfunn bedre i stand til å ivareta våre forpliktelser i det internasjonale politisamarbeidet på en langt bedre måte enn det som er tilfelle i dag.

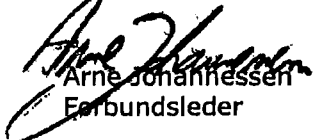
Gjennom menneskerettskonvensjonen har Norge forpliktet seg til å sikre politiet effektive etterforskningsverktøy for å kunne bekjempe kriminalitet og derved ivareta borgernes menneskerettigheter. PF ønsker å uttrykke bekymring for at dersom ikke datalagringsdirektivet gjennomføres, vil dette kunne få store konsekvenser for politiet og samfunnets muligheter til å bekjempe kriminalitet. Vi mener at det kun er et tidsspørsmål før tilbyderne ikke lenger har behov for oppbevaring av trafikkdata i faktureringsøyemed. Politiet risikerer da å miste ett av sine viktigste verktøy, noe som vil ha alvorlig konsekvenser og kunne gå på bekostning av både demokratiet og rettssikkerheten i samfunnet.

Vi ønsker å oppsummere høringsnotatet med følgende punkter:

- Tiden "overmoden" for en regulering av praksisen rundt datalagring. Dette må videre sees i et samfunnsmessig perspektiv, hvor behov for trygghet og bekjempelse av alvorlig og organisert kriminalitet bør bli vektlagt.
- **Personvernet** vil bli styrket gjennom en implementering av datalagringsdirektivet, nettopp fordi slike opplysninger stadig oftere benyttes i etterforskningen og er avgjørende for å bevise både skyld og uskyld.
- Personvernet og rettssikkerheten er viktig for alle, også for barna som blir utsatt for overgrep. Et nei til direktivet vi vil styrke de kriminelle sitt personvern og svekke de svakeste.
- Data knyttet til internettbruk slettes nå etter 3 uker etter pålegg fra Datatilsynet. Dette pålegget endret og minsket politiets mulighet til å etterforske internettrelatert kriminalitet betraktelig, spesielt mht internettrelaterte seksuelle overgrep mot barn.
- EU's datalagringsdirektiv legger opp til et godt, helhetlig rammeverk for håndtering av denne trafikkdata. PF mener at direktivet vil sikre et bedre personvern enn det som er tilfellet i dag, hvor trafikkdata blir lagret utelukkende på grunnlag av teletilbydernes kommersielle behov.
- Dagens lovverk er i uttakt med kriminalitetsutviklingen. En opprettholdelse av dagens regelverk er en trussel mot rettssikkerheten.
- For samfunnet er bruken av trafikkdata et av de viktigste verktøyene i bekjempelsen av organisert og annen alvorlig kriminalitet. Datalagringsdirektivet vil gjøre politiet bedre i stand til å kunne bekjempe organisert og alvorlig kriminalitet på en god og effektiv måte, for samfunnets beste.
- Ekomloven bør endres slik at trafikkdata kan innhentes vederlagsfritt fra teletilbyderne. I et samfunnsøkonomisk perspektiv vil være både ressursbesparende og effektivt. Alternativt bør det innføres en sentral refusjonsordning lik den som finnes i dag for sikring av DNA spor og analyser av disse.
- Intensjonen med Datalagringsdirektivet om å gjøre politiet bedre i stand til å bekjempe alvorlig og organisert kriminalitet, kan bli undergravet om en innfører krav om strafferamme på fengsel i tre år eller mer.

- Datalagringsdirektivet legger et godt grunnlag for kontroll, og vil gjøre norsk politi og samfunn bedre i stand til å ivareta våre forpliktelser i det internasjonale politisamarbeidet på en langt bedre måte enn det som er tilfelle i dag.
- Ideelt sett bør man fastslå en lagringstid på to år, og minimum ett år. Dette vil gjøre politiet bedre i stand til å kunne bekjempe organisert og alvorlig kriminalitet på en god og effektiv måte, for samfunnets beste.
- Det er kun et tidsspørsmål før tilbyderne ikke lenger har behov for oppbevaring av trafikkdata i faktureringsøyemed. Politiet risikerer da å miste ett av sine viktigste verktøy, noe som vil ha alvorlig konsekvenser og kunne gå på bekostning av både demokratiet og rettssikkerheten i samfunnet.

Med vennlig hilsen



Arne Johannessen
Forbundsleder



Anne-Catherine Gustafson
Forbundssekretær

Kopi:
Justisminister Knut Storberget
Justiskomiteen
Politidirektør
UNIO