DET KONGELIGE
JUSTIS- OG BEREDSKAPSDEPARTEMENT

Prop. 31 L

(2022–2023)

Proposisjon til Stortinget (forslag til lovvedtak)

Endringer i politiloven og politiregisterloven (PSTs etterretningsoppdrag og bruk av åpent tilgjengelig informasjon)

DET KONGELIGE
JUSTIS- OG BEREDSKAPSDEPARTEMENT

Prop. 31 L

(2022–2023)

Proposisjon til Stortinget (forslag til lovvedtak)

Endringer i politiloven og politiregisterloven (PSTs etterretningsoppdrag og bruk av åpent tilgjengelig informasjon)

Innhold

DET KONGELIGE
JUSTIS- OG BEREDSKAPSDEPARTEMENT

Prop. 31 L

(2022–2023)

Proposisjon til Stortinget (forslag til lovvedtak)

Endringer i politiloven og politiregisterloven (PSTs etterretningsoppdrag og bruk av åpent tilgjengelig informasjon)

Tilråding fra Justis- og beredskapsdepartementet 2. desember 2022, godkjent i statsråd samme dag.
(Regjeringen Støre)

1 Proposisjonens hovedinnhold

I denne proposisjonen foreslås det endringer i politiloven og politiregisterloven.

For det første foreslås det endringer i politiloven som lovfester Politiets sikkerhetstjenestes (PSTs) oppgave som innenlands etterretningstjeneste, og som tydeliggjør hva denne oppgaven innebærer. Det er i en rekke sammenhenger forutsatt og forventet at PST skal ha denne rollen allerede i dag, men oppdraget og hva det innebærer, er ikke tilstrekkelig reflektert i dagens lovverk. Dette gjør at PST ikke har mulighet til å oppfylle de forventninger som stilles til tjenesten. Oppgaven som innenlands etterretningstjeneste foreslås formulert som at PST skal utarbeide analyser og etterretningsvurderinger om forhold i Norge som kan true Norges suverenitet, territorielle integritet, demokratiske styreform og andre nasjonale sikkerhetsinteresser. Analysene og etterretningsvurderingene vil være rådgivende, og er ment å utgjøre beslutningsstøtte for å prioritere innsatsområder, ressurser og tiltak. Ved begrensningen til forhold «i Norge» avgrenses oppgaven mot de som tilligger Etterretningstjenesten (E-tjenesten). Det foreslås også en klar hjemmel i politiregisterloven for at PST kan behandle opplysninger som er nødvendige for dette formålet. Dette vil gjøre at PST kan behandle opplysninger i et noe større omfang enn det tjenesten gjør i dag. Forslaget omtales nærmere i proposisjonens punkt 7.

For det andre foreslås det å åpne for at PST kan lagre, systematisere og analysere store mengder åpent tilgjengelig informasjon til etterretningsformål, selv om den enkelte opplysning isolert sett ikke er nødvendig for dette formålet. Det er et vilkår at behandlingen antas å være nødvendig for utarbeidelse av analyser og etterretningsvurderinger. Begrunnelsen for forslaget er at det etter departementets syn er nødvendig å åpne for denne typen behandling for at PST skal kunne ivareta oppgaven som innenlands etterretningstjeneste og oppfylle forventningen om at de skal

«følge med» på internett. Forslaget vil være avgjørende for at PST skal kunne analysere endringer i trusselbildet og vil bidra til at PST kan avdekke ukjente trusselaktører og oppdage nye fenomener som kan medføre nye trusler.

Med åpent tilgjengelig informasjon menes informasjon som er allment tilgjengelig for offentligheten. Som en sentral sikkerhetsmekanisme foreslås det at den lagrede informasjonen skal sperres. Dette innebærer at opplysningene bare kan brukes til de konkret angitte formålene, og at opplysningene ellers ikke anses å være registrert hos PST. Opplysningene skal holdes atskilt fra opplysninger som ellers behandles hos PST. I tillegg til bruk til utarbeidelse av analyser og etterretningsvurderinger, foreslås det å åpne for at PST kan bruke opplysningene i forebyggende sak og i etterforskingen av straffbare handlinger innenfor PSTs ansvarsområde. Opplysningene skal slettes senest etter fem år, men med en mulighet for å beslutte fortsatt lagring på nærmere vilkår. Forslaget omtales nærmere i proposisjonens punkt 8.

2 Bakgrunn og behovet for endringer

2.1 Lovfesting av PSTs etterretningsoppdrag

Dagens bestemmelser om PSTs oppdrag i politiloven ble vedtatt rundt årtusenskiftet. Siden den gang er trusselbildet vesentlig endret.

Trusselbildet er blant annet beskrevet av Justis- og beredskapsdepartementet i Prop. 1 S (2022–2023), punkt 1.6.2 side 19 til 20:

> «Trusselbiletet mot den nasjonale tryggleiken er komplekst og karakterisert ved mindre føreseielege truslar frå både framande statar, organiserte kriminelle nettverk og terroristar. Dei tradisjonelle tryggleiksutfordringane er endra, på same tid som nye er komne til. Kombinasjonen av ulike verkemiddel, sivile og militære, opne og fordekte, i det fysiske så vel som i det digitale rommet, gjer trusselbiletet utfordrande og samansett.
>
> Politiets tryggingsteneste ventar framleis at trusselen frå ekstrem islamisme og høgreekstremisme vil utgjere dei største terrortruslane mot Noreg. Dei er òg bekymra for auka negativ merksemd mot norske styresmaktpersonar frå ekstremistar.
>
> Samansett verkemiddelbruk omfattar både operasjonar i det digitale rommet og meir konvensjonelle tiltak, irekna det som ved første augekast kan sjå ut som ordinær kriminalitet i form av bl.a. skadeverk eller grovt tjuveri. Økonomiske tiltak, oppkjøp, falske nyheiter og ulike former for påverknadsoperasjonar er metodar som er særleg krevjande å møte. Samansett verkemiddelbruk utfordrar evna styresmaktene har til å fange opp trusselaktørar. Desse utfordringane er eit døme på at arbeidet med nasjonal tryggleik krev eit breitt samarbeid på tvers av sektorane i Noreg. Det er òg viktig at dei nasjonale tryggingsstyresmaktene har tilstrekkeleg heimelsgrunnlag, kompetanse og ressursar til å avdekke, motverke og handtere den breie verkemiddelbruken som framande statar rettar mot Noreg. Regjeringa vurderer behovet for regelverkstiltak.
>
> Det er grunn til å tru at cyberoperasjonar som metode for bl.a. etterretning og påverknad vil vere særs aktuelt framover, og dette er forsterka av den nye tryggleikspolitiske situasjonen som Russland sitt angrep på Ukraina har skapt, då slike operasjonar vil kunne gi høg effekt utan stor risiko for den som står bak. Vidare har Russland vist ei evne til å bruke heile verkemiddelapparatet til staten for å oppnå politiske mål, gjennom såkalla samansett verkemiddelbruk. Fleire forhold kan påverke viljen Russland har til å utnytte slike verkemiddel, t.d. vestlege sanksjonar.»

Den sikkerhetspolitiske situasjonen i Europa er forandret etter Russlands invasjon av Ukraina og har også ført til en økt etterretningstrussel mot Norge. Også skytingen i Oslo 25. juni i år, som PST på det nåværende tidspunkt vurderer som en ekstrem islamistisk terrorhandling, aktualiserer behovet for kontinuerlig å følge med på trusselbildet også knyttet til radikalisering og terror.

PSTs oppdrag etter politiloven er i hovedsak beskrevet som forebygging og etterforsking av konkret angitte straffbare handlinger. Etter politiregisterlovens regler kan tjenesten behandle opplysninger som er nødvendige for disse oppgavene. Slik PSTs oppgaver er beskrevet i dag, er tjenestens mulighet til å behandle informasjon for å bidra med generelle etterretningsvurderinger og analyser knyttet til trender og utvikling i trusselbildet, begrenset. PSTs trusselvurderinger baserer seg i dag hovedsakelig på informasjon fra konkrete enkeltsaker, forskning og informasjon fra samarbeidene tjenester, altså i stor grad historisk informasjon. Dersom PST skal evne å gi relevant og rettidig informasjon og beslutningsstøtte om nåsituasjonen og fremtidig trusselbilde innenfor sitt ansvarsområde, må tjenesten ha et bredere informasjonstilfang å bygge sine vurderinger på. Det er derfor etter departementets vurdering nødvendig at det lovfestes i politiloven at PST er en innenlands etterretningstjeneste, og hva som ligger i denne oppgaven må reguleres nærmere. I tillegg må det gis hjemmel og regler for å behandle opplysninger også for dette formålet. Disse end-

ringene vil legge til rette for at alle typer informasjon, herunder informasjon fra åpne kilder, vil kunne behandles til rene etterretningsformål.

Det at PSTs oppgave som innenlands etterretningstjeneste ikke eksplisitt fremgår av eller spesifiseres i regelverket, gjør også at PSTs og E-tjenestens mandat ikke fullt ut utfyller hverandre. Det innebærer en risiko for at det oppstår et gap mellom det PST arbeider med og det E-tjenesten arbeider med. Dette kan medføre etterretningssvikt og manglende beslutningsstøtte på områder som kan ha betydning for nasjonale sikkerhetsinteresser. At mandatene ikke fullt ut utfyller hverandre kan også være et hinder for informasjonsutveksling, ved at PST ikke nødvendigvis vil ha hjemmel til å behandle opplysninger som E-tjenesten ønsker å utlevere til PST. Dette kan for eksempel omfatte informasjon om forhøyet aktivitet og interesse fra enkelte nasjoner i Nord-Norge, som oppkjøp av eiendom, konsesjonssøknader mv., der det ikke foreligger bekymring for noe straffbart. Informasjonen kan likevel være viktig for å forstå endringer fra normalbildet, som igjen kan avdekke en ny trend eller trussel.

2.2 Utvidet bruk av åpent tilgjengelig informasjon

Som beskrevet ovenfor, har den digitale hverdagen medført store endringer i trusselbildet. Den teknologiske og samfunnsmessige utviklingen medfører dessuten at trusselaktørene i økende grad flytter sin aktivitet fra det fysiske til det digitale rom. Internett benyttes i økende grad til planlegging og gjennomføring av trusler fra statlige og ikke-statlige aktører, og kan også være en arena for radikalisering og kunnskapsdeling som kan øke trusselen ytterligere. Dette gjør at PST må arbeide på nye måter for å håndtere de aktuelle truslene, herunder gjennom bruk av nye virkemidler som er tilpasset den digitale utviklingen. Når de ytre omstendighetene i samfunnet endres, må også måten etterretning bedrives på tilpasses endringene. PST har det samme ansvaret i det digitale rom som i den fysiske verden. Det er departementets syn at tjenesten må ha de nødvendige verktøyene for å ivareta dette ansvaret.

Behovet for og ønsket om at PST skal «følge med» på internett er ikke nytt. I NOU 2012: 14 Rapport fra 22. juli-kommisjonen punkt 16.6 side 391 om åpne kilder og overvåking av internett står det:

> «PST bør ikke la bekymringen for å bli beskyldt for politisk overvåking stå i veien for å følge med på ekstremistiske nettsider, og gjøre registreringer om noen framsetter trusler eller andre ytringer som gir grunnlag til mistanke.»

Kommisjonen la til grunn at det å følge med på om noen ytrer seg truende i diskusjoner i fora med ekstreme meninger, kan følges opp gjennom en åpen tilstedeværelse og innhenting av informasjon fra internett.

Uttalelsene er fulgt opp i Meld. St. 21 (2012–2013) Terrorberedskap – Oppfølging av NOU 2012: 14 Rapport fra 22. juli-kommisjonen, der det i punkt 6.5.7 side 53 om informasjon innhentet ved bruk av åpne kilder er uttalt:

> «Kommisjonen gir uttrykk for en forventning om at PST skal 'følge med' på ekstremistiske nettsider. Det betyr i praksis å følge med på hva folk foretar seg på internett. Kommisjonen problematiserer ikke om det som følge av dette vil skje registrering eller annen politisk overvåkning. Utgangspunktet er likevel helt klart. Skal PST følge med på internett vil det kunne innebære en større grad av overvåkning på nettet. Å følge med vil i praksis si å registrere informasjon om enkeltpersoner og grupper og deres ytringer. For å kunne være av verdi i etterretningsarbeidet må informasjonen deretter kunne lagres og være gjenfinnbar.»

I rapporten «Evaluering av politiets og PSTs håndtering av terrorhendelsen i Bærum 10. august 2019» beskrives en utvikling etter 22. juli 2011 i trusselbildet fra høyreekstreme som i stor grad har skjedd på nett, både i åpne og lukkede fora.

PST har i sine åpne trusselvurderinger over flere år påpekt at aktivitet på digitale plattformer og digitale nettverk er av stor betydning for utviklingen i trusselbildet på en rekke områder innenfor PSTs mandat. I PSTs nasjonale trusselvurdering for 2022 uttales det på side 7, 12 og 16 at nettverksoperasjoner fremdeles vil utgjøre en alvorlig trussel mot Norge, at internett er en stadig viktigere arena for informasjonsinnhenting for fremmede etterretningstjenester og at digitale plattformer fremdeles vil være de viktigste arenaene for radikalisering til høyreekstremisme. Det omtales på side 19 at trusselen fra ekstreme islamister primært vil komme fra personer som deltar i ekstremistiske digitale nettverk.

Det er ikke tvilsomt at PST allerede i dag har anledning til å behandle informasjon fra åpne kilder når behandlingen er knyttet til tjenestens opp-

drag slik det er definert i politiloven, og vilkårene for behandling av opplysningene etter politiregisterloven er oppfylt. Dersom det stadfestes i politiloven at PST også har mandat som en innenlands etterretningstjeneste, vil det imidlertid være nødvendig for tjenesten å lagre, systematisere og analysere større mengder åpent tilgjengelig informasjon for å ivareta oppgaven fullt ut. For å kunne kartlegge og «følge med» på utviklingen i digitale trusler og endringer i trusselbildet, er det videre behov for å kunne lagre informasjonen over tid. Politiregisterlovens alminnelige regler om behandling av opplysninger åpner i dag ikke for denne typen behandling.

3 Høringen

Forslag til endringer i politiloven og politiregisterloven ble sendt på høring 7. oktober 2021, med høringsfrist 7. januar 2022. Høringsnotatet ble sendt til følgende instanser:

Departementene

Arbeids- og velferdsdirektoratet
Arbeidstilsynet
Arkivverket
Barneombudet
Barne-, ungdoms- og familiedirektoratet
Datatilsynet
Digitaliseringsdirektoratet
Direktoratet for forvaltning og økonomistyring
Direktoratet for samfunnssikkerhet og beredskap
Domstoladministrasjonen
Etterretningstjenesten
Forbrukerombudet
Forsvarsstaben
Helsedirektoratet
Integrerings- og mangfoldsdirektoratet
Kommisjonen for gjenopptakelse av straffesaker
Kontrollutvalget for kommunikasjonskontroll
Kriminalomsorgsdirektoratet
Kripos
Likestillings- og diskrimineringsombudet
Luftfartstilsynet
Nasjonal kommunikasjonsmyndighet
Nasjonal sikkerhetsmyndighet
Norges institusjon for menneskerettigheter (NIM)
Personvernkommisjonen
Politidirektoratet
Politihøgskolen
Politiets sikkerhetstjeneste (PST)
Regelrådet for næringslivet
Regjeringsadvokaten
Riksadvokaten
Sametinget
Sivil klareringsmyndighet
Sivilombudet
Skattedirektoratet
Spesialenheten for politisaker
Statens sivilrettsforvaltning
Statistisk Sentralbyrå
Statsadvokatembetene
Stortingets kontrollutvalg for etterretnings-, overvåkings- og sikkerhetstjeneste (EOS- utvalget)
Sysselmesteren på Svalbard
Tolldirektoratet
Utlendingsdirektoratet
Utlendingsnemnda
Vegdirektoratet
ØKOKRIM

Amnesty International Norge
Antirasistisk Senter
Den Norske Advokatforening
Den Norske Dommerforening
Finansnæringens Fellesorganisasjon
Innvandrernes landsorganisasjon
Juridisk rådgivning for kvinner (JURK)
Jussbuss
Jussformidlingen
Kommunesektorens organisasjon
Landsorganisasjonen i Norge (LO)
Mediebedriftenes landsforening
Norges politilederlag
Norsk forening for kriminalreform
Norsk Journalistlag
Norsk Presseforbund
Norsk Redaktørforening
Næringslivets Hovedorganisasjon
OMOD (Organisasjon mot offentlig diskriminering)
Politiets Fellesforbund
Tekna
Redd Barna, Rettighetssenteret
Rettspolitisk forening
Røde kors
Samarbeidsrådet for tros- og livssynssamfunn
Stiftelsen for en Kritisk og Undersøkende Presse

Det juridiske fakultet ved Universitetet i Oslo
Det juridiske fakultet ved Universitetet i Bergen
Det juridiske fakultet ved Universitetet i Tromsø
Forsvarets forskningsinstitutt
Forsvarets høgskole
Institutt for forsvarsstudier
Institutt for fredsforskning (PRIO)

Norsk Utenrikspolitisk Institutt (NUPI)

Følgende instanser hadde merknader til høringsnotatet:

Forsvarsdepartementet

Datatilsynet
Det nasjonale statsadvokatembetet
Digitaliseringsdirektoratet
Direktoratet for samfunnssikkerhet og beredskap
Stortingets kontrollutvalg for etterretnings-, overvåkings- og sikkerhetstjeneste (EOS-utvalget)
Finnmark politidistrikt
Kripos
Medietilsynet
Nasjonal kommunikasjonsmyndighet
Norges institusjon for menneskerettigheter
Oslo statsadvokatembeter
Politidirektoratet
Politiets sikkerhetstjeneste
Riksadvokaten

Advokatforeningen
Den Norske Dataforening
Elektronisk Forpost Norge
IKT-Norge
NITO
Rettspolitisk forening
Tekna
UTSYN

I tillegg har om lag 20 privatpersoner avgitt høringsinnspill.

Følgende instanser har meldt at de ikke har merknader eller ikke ønsker å uttale seg om forslaget:

Helse- og omsorgsdepartementet
Landbruks- og matdepartementet
Samferdselsdepartementet

Domstolsadministrasjonen
Generaladvokatembetet
Helsedirektoratet
Kriminalomsorgsdirektoratet
Skattedirektoratet
Statistisk sentralbyrå
Tolldirektoratet

4 Gjeldende rett

4.1 Politiloven

PSTs oppgaver er regulert i politiloven kapittel III a. Det fremgår av politiloven § 17 a at oppgavene nevnt i § 17 b utføres av et eget politiorgan, som ledes av en sentral enhet.

Hvilke straffbare forhold PST skal forebygge og etterforske er regulert i politiloven § 17 b. PST skal blant annet forebygge og etterforske følgende straffbare handlinger som kan true rikets sikkerhet: Overtredelser av straffeloven kapittel 17 (bestemmelser om vern av Norges selvstendighet og andre grunnleggende nasjonale interesser), av § 184 (krenkelsene av representasjonen til en fremmed stat eller mellomstatlig organisasjon) og av sikkerhetsloven, ulovlig etterretningsvirksomhet, sabotasje og politisk motivert vold eller tvang samt overtredelser av straffeloven §§ 131 til 136 b, 145 eller 146 (terrorlovbrudd mv.).

Enkelte særlige oppgaver for den sentrale enhet i PST (heretter DSE) er regulert i politiloven § 17 c. DSE skal etter denne bestemmelsen utarbeide trusselvurderinger til bruk for politiske myndigheter, samarbeide med andre lands politimyndigheter og sikkerhets- og etterretningstjenester og foreta personkontroll til bruk ved sikkerhetsundersøkelser.

Instruks 19. august 2005 nr. 920 for Politiets sikkerhetstjeneste, gitt med hjemmel i politiloven § 29, fastsetter nærmere regler om PSTs oppgaver og virksomhet, jf. instruksen § 1. Det fremgår av § 5 første ledd at tjenesten skal utføre sine forebyggende oppgaver ved blant annet å innhente, bearbeide, analysere og utveksle informasjon i samsvar med fastsatte prioriteringer. Det fremgår av § 6 første ledd at tjenesten av eget tiltak eller etter anmodning fra Justis- og beredskapsdepartementet, skal *«utarbeide trusselvurderinger og gi råd om tiltak av betydning for norske interesser, virksomheter og enkeltpersoners sikkerhet»*.

4.2 Politiregisterloven og politiregisterforskriften

Politiregisterloven og politiregisterforskriften regulerer politiets og påtalemyndighetens behandling av opplysninger. Behandling av opplysninger defineres i politiregisterloven § 2 nr. 2 som enhver elektronisk eller manuell bruk av opplysninger, og omfatter blant annet innsamling, registrering, systematisering, strukturering og oppbevaring av opplysningene.

Regelverket gjennomfører direktiv (EU) 2016/680 om behandling av personopplysninger i kriminalitetsbekjempende øyemed. Direktivets virkeområde omfatter ikke aktiviteter som faller utenfor unionsretten, herunder aktivitetene til de nasjonale etterretningstjenestene, jf. artikkel 2 nr. 3 bokstav a. Siden PST er en del av politiet, er politiregisterloven, og derved også en rekke av direktivets bestemmelser, likevel gitt anvendelse for PST. Det er imidlertid gitt en rekke særbestemmelser for tjenesten som reflekterer at PSTs virksomhet skiller seg fra virksomheten til det øvrige politiet. For det første gjelder politiregisterloven, i motsetning til for det øvrige politiet, også for PSTs forvaltningsvirksomhet, jf. politiregisterloven § 3 annet ledd. Videre er det i lovens kapittel 11 gitt en rekke særbestemmelser for PST. De største forskjellene sammenlignet med politiet for øvrig finnes i §§ 64, 66 og 68 om henholdsvis nødvendighetskravet, informasjonsplikt, innsyn og tilsyn. For PSTs behandling av opplysninger utenfor den enkelte straffesak er nødvendighetskravet knyttet til beskrivelsen av PSTs arbeidsoppgaver etter politiloven §§ 17 b og 17 c og adgangen til å bruke forebyggende tvangsmidler etter § 17 d, slik at PST kan behandle opplysninger som er nødvendige for disse oppgavene. For behandling av opplysninger i PSTs straffesaker gjelder straffeprosesslovens regler på vanlig måte. PST kan opprette såkalt «forebyggende sak» dersom det er grunn til å undersøke om noen forbereder et lovbrudd som PST har til oppgave å forebygge, jf. politiregisterloven § 64 tredje ledd nr. 1 bokstav a og definisjonen i politiregisterforskriften § 20-3 nr. 2.

Bestemmelsene om informasjonsplikt og innsyn i politiregisterloven §§ 48 og 49 gjelder ikke for PST, jf. § 66. Tilsynsorganet for PST er EOS-utvalget, jf. § 68, mens denne funksjonen tilligger Datatilsynet for det øvrige politiet. EOS-utvalgets kontroll med PST er nærmere regulert i lov 3. februar 1995 nr. 7 om kontroll med etterretnings-, overvåkings- og sikkerhetstjeneste (EOS-kontrolloven). EOS-utvalget skal sikre at virksomheten holdes innenfor rammen av tjenestens fastlagte oppgaver og føre kontroll med tjenestens behandling av forebyggende saker og etterforskingssaker, dens bruk av skjulte tvangsmidler og andre skjulte metoder for informasjonsinnhenting, jf. EOS-kontrolloven § 6 fjerde ledd nr. 1. Utvalget mottar også klager fra enkeltpersoner eller organisasjoner, og skal av eget tiltak ta opp alle saker og forhold som det ut fra formålet finner riktig å behandle, jf. EOS-kontrolloven § 5.

Både PST og politiet for øvrig er gitt anledning til å behandle opplysninger i inntil fire måneder dersom det er nødvendig for å avklare om kravene til formålsbestemthet, nødvendighet og relevans er oppfylt, jf. §§ 65 og 8. Opplysningene skal snarest mulig underlegges kontroll, slik at de enten slettes eller behandles etter annet rettslig grunnlag. Som ledd i kontrollen kan opplysningene gjøres kjent for andre tjenestemenn i politiet og påtalemyndigheten. Opplysningene kan også utleveres til andre dersom det er strengt nødvendig for kontrollen. Tidsfristen på fire måneder er absolutt, men gjelder ikke behandling av opplysninger i den enkelte straffesak, jf. § 8 tredje ledd.

Politiregisterloven åpner for at opplysninger som behandles av politiet og påtalemyndigheten kan *sperres.* Sperring innebærer *«markering av lagrede opplysninger i den hensikt å begrense den fremtidige behandlingen av disse opplysningene»,* jf. § 2 nr. 10. Når opplysninger sperres må det alltid samtidig fremgå hvilke formål de sperrede opplysningene kan brukes til. Det må videre skilles mellom de tilfellene der sperring er et substitutt for sletting, og de tilfellene der hensikten med sperring kun er å begrense formålet med behandlingen av opplysningene. Dersom sperring er et substitutt for sletting, fremgår det av § 52 at sperrede opplysninger bare kan brukes til det formål som gjorde at opplysningen ikke ble slettet. Ett eksempel på dette er § 51 annet og tredje ledd om sletting og sperring av opplysninger med feil eller mangler. Opplysninger som er beheftet med feil som ikke kan repareres, skal slettes eller sperres. Dersom opplysningene sperres, kan de bare brukes til dokumentasjon. Her vil det være et absolutt forbud mot å bruke de sperrede opplysningene til andre formål. Dersom hensikten med sperringen bare er å begrense den fremtidige bruken av opplysningene, vil adgangen til å bruke opplysningene bero på en tolkning av de angitte formålene.

Videre følger det av politiregisterforskriften § 15-2 annet ledd at opplysninger som er sperret, skal holdes atskilt. Tilgangen til opplysninger som er sperret skal begrenses til så få personer som mulig, og skal bare gis til personer som har fått særskilt bemyndigelse. Slik bemyndigelse skal bare gis til kvalifiserte personer som har gjennomgått opplæring, jf. politiregisterforskriften § 8-4 annet ledd.

Supplerende regler for PSTs behandling av opplysninger finnes i politiregisterforskriften del 6. I forskriften kapittel 20 er det gitt generelle bestemmelser, herunder om formålet med behandlingen. Kapittel 21 inneholder særlige bestemmelser om behandling av opplysninger, der det blant annet er gitt nærmere presiseringer av nødvendighetskriteriet. Videre er det bestemmelser om hvem det kan registreres opplysninger om og hvilke opplysninger som kan behandles om den enkelte. Kapittelet inneholder også regler om opprettelse av og behandling av opplysninger i forebyggende sak, jf. § 21-5. Blant annet skal Sjef PST eller den han bemyndiger, godkjenne opprettelsen, det kan bare behandles opplysninger som har saklig tilknytning til saken, og saken skal gjennomgås hvert år for vurdering av om den skal avsluttes eller videreføres. Kapittel 22 gir regler om informasjonsplikt, innsyn, retting, sperring og sletting. Kapittel 23 gjelder informasjonssikkerhet og internkontroll.

4.3 Lov om Etterretningstjenesten

Lov 19. juni 2020 nr. 77 om Etterretningstjenesten (etterretningstjenesteloven) regulerer E-tjenestens virksomhet og oppgaver. Loven skal blant annet bidra til å trygge Norges suverenitet, territorielle integritet, demokratiske styreform og andre nasjonale sikkerhetsinteresser, herunder forebygge, avdekke og motvirke utenlandske trusler mot Norge og norske interesser, jf. § 1-1 første ledd bokstav a. Det følger av Prop. 80 L (2019–2020) Lov om Etterretningstjenesten (etterretningstjenesteloven) kapittel 17 side 193 at begrepene skal forstås på samme måte som i lov 1. juni 2018 nr. 24 om nasjonal sikkerhet (sikkerhetsloven).

I etterretningstjenesteloven § 2-1 første ledd første punktum fremgår det eksplisitt at E-tjenesten er Norges nasjonale utenlandsetterret-

ningstjeneste. Tjenestens oppgaver er angitt i kapittel 3, der det blant annet fremgår av § 3-1 at E-tjenesten skal «*innhente og analysere informasjon om utenlandske forhold som kan bidra til å avdekke og motvirke*» nærmere angitte trusler, herunder trusler mot Norges selvstendighet og sikkerhet, territorielle integritet og politiske og økonomiske handlefrihet, alvorlige trusler mot samfunnssikkerheten i Norge, alvorlige trusler mot norske interesser i utlandet og fremmed etterretningsvirksomhet.

Lovens kapittel 5 oppstiller grunnvilkår for innhenting og utlevering av informasjon. Etter § 5-3 kan E-tjenesten innhente *rådata i bulk* når det er nødvendig for å få tilgang til et relevant og tilstrekkelig informasjonsgrunnlag. Bestemmelsen oppstiller videre vilkår for å kunne søke i det innhentede materialet. Med *rådata* menes «*ubearbeidet eller automatisk bearbeidet informasjon i enhver form hvis etterretningsverdi ikke er vurdert*», mens *bulk* er «*informasjonssamlinger og datasett hvorav en vesentlig andel av informasjonen antas å være irrelevant for etterretningsformål*», jf. § 1-3 bokstav h og i. Innhenting av informasjon i bulk kan gjøres gjennom enhver innhentingsmetode, herunder fra åpne kilder. Etter § 9-8 skal rådata i bulk slettes senest etter 15 år, men med mulighet for utsatt sletting i inntil fem år av gangen dersom vesentlige hensyn tilsier det. Beslutning om utsatt sletting treffes av sjefen for E-tjenesten.

Lovens kapittel 6 regulerer metoder for innhenting av informasjon som kan medføre inngrep overfor den enkelte. Etter § 6-2 kan E-tjenesten innhente åpent tilgjengelig informasjon. Det fremgår av bestemmelsens annet punktum at informasjon ikke er åpent tilgjengelig dersom tilgang krever aktiv fordekt opptreden eller forsering av passord eller lignende beskyttelsesmekanismer.

En særlig form for bulkinnhenting er regulert i lovens kapittel 7 og 8, som åpner for at E-tjenesten på nærmere vilkår kan innhente elektronisk kommunikasjon som transporteres over den norske grensen (tilrettelagt innhenting av grenseoverskridende elektronisk kommunikasjon). Dette innebærer at E-tjenesten kan innhente og lagre store mengder metadata om elektronisk kommunikasjon som krysser den norske grensen. Søk i lagrede metadata krever kjennelse fra retten, og tjenesten kan ikke innhente og lagre innholdsdata før retten har godkjent det. Bestemmelsene kommer bare til anvendelse der det er nødvendig at ekomtilbydere mv. legger til rette for innhentingen, jf. §§ 7-1 og 7-2.

5 Rettslige rammer

5.1 Retten til privatliv – Grunnloven § 102 og EMK artikkel 8

Både nasjonale og internasjonale regler har betydning for utformingen av regler om håndtering av personopplysninger. For det første har Grunnloven § 102 regler som verner privatlivet. I det internasjonale regelverket er Den europeiske menneskerettskonvensjonen 4. november 1950 (EMK) av særlig betydning. Konvensjonen er gjennom menneskerettsloven 21. mai 1999 nr. 30 gjort til norsk lov, og går foran annen norsk lovgivning ved motstrid, jf. menneskerettsloven § 3. Retten til privatliv beskyttes også av FNs konvensjon om økonomiske, sosiale og kulturelle rettigheter (SP) artikkel 17.

5.1.1 I hvilken grad utgjør behandling av informasjon fra åpne kilder et inngrep i privatlivet?

Grunnloven § 102 lyder:

> «Enhver har rett til respekt for sitt privatliv og familieliv, sitt hjem og sin kommunikasjon. Husransakelse må ikke finne sted, unntatt i kriminelle tilfeller.
>
> Statens myndigheter skal sikre et vern om den personlige integritet.»

Bestemmelsen kom inn i Grunnloven som ledd i grunnlovsreformen i 2014. Komiteen ga i Innst. 186 S (2013–2014) punkt 2.1.9 side 27 uttrykk for at bestemmelsen gir rett til et vern av personopplysninger ved at den «*skal leses som at systematisk innhenting, oppbevaring og bruk av opplysninger om andres personlige forhold bare kan finne sted i henhold til lov, benyttes i henhold til lov eller informert samtykke og slettes når formålet ikke lenger er til stede*».

Grunnloven § 102 åpner etter sin ordlyd ikke for å gjøre unntak fra eller inngrep i retten til privatliv. Høyesterett har imidlertid lagt til grunn at bestemmelsen har klare likhetstrekk med EMK artikkel 8 og må tolkes i lys av denne, jf. blant annet HR-2020-2372-A avsnitt 38. Dette innebærer at inngrep i retten til privatliv kan være forenlig med Grunnloven § 102, såfremt inngrepet har tilstrekkelig hjemmel, forfølger et legitimt formål og er forholdsmessig, se Rt. 2014 side 1105 avsnitt 28 og Rt. 2015 side 93 avsnitt 60.

EMK artikkel 8 lyder i norsk oversettelse:

> «1. Enhver har rett til respekt for sitt privatliv og familieliv, sitt hjem og sin korrespondanse.
> 2. Det skal ikke skje noe inngrep av offentlig myndighet i utøvelsen av denne rettighet unntatt når dette er i samsvar med loven og er nødvendig i et demokratisk samfunn av hensyn til den nasjonale sikkerhet, offentlige trygghet eller landets økonomiske velferd, for å forebygge uorden eller kriminalitet, for å beskytte helse eller moral, eller for å beskytte andres rettigheter og friheter.»

Kjernen i bestemmelsen er at den enkelte har krav på respekt for sitt privatliv, sitt hjem og sin korrespondanse. Den europeiske menneskerettsdomstolen (EMD) har i flere avgjørelser fastslått at EMK artikkel 8 også innebærer en rett til vern av personopplysninger, se for eksempel *Leander mot Sverige* 26. mars 1987. I den forbindelse har EMD uttalt at begrepet «privatliv» skal tolkes vidt i lys av Europarådets konvensjon fra 1981 om elektronisk behandling av personopplysninger, hvor personopplysninger er definert som «*enhver opplysning som gjelder en bestemt eller identifiserbar enkeltperson*», se *Satakunnan Markkinapörssi Oy og Satamedia Oy mot Finland* 27. juni 2017 avsnitt 133.

Flere avgjørelser fra EMD gir anvisning på at innsamling og behandling av offentlig tilgjengelig informasjon vil kunne innebære et inngrep i privatlivet etter EMK artikkel 8 nr. 1. I *P.G. og J.H. mot Storbritannia* 25. september 2001, heter det i avsnitt 56: *«There is therefore a zone of interaction of a person with others, even in a public context, which may fall within the scope of «private life».»* Videre følger det av avsnitt 57:

> «There are a number of elements relevant to a consideration of whether a person's private life is concerned by measures effected outside a person's home or private premises. Since there are occasions when people knowingly or intentionally involve themselves in activities which are or may be recorded or reported in a public manner, a person's reasonable expectations as to privacy may be a significant, although not necessarily conclusive, factor. A person who walks down the street will, inevitably, be visible to any member of the public who is also present. Monitoring by technological means of the same public scene (for example, a security guard viewing through closed-circuit television) is of a similar character. Private-life considerations may arise, however, once any systematic or permanent record comes into existence of such material from the public domain. It is for this reason that files gathered by security services on a particular individual fall within the scope of Article 8, even where the information has not been gathered by any intrusive or covert method (see Rotaru v. Romania [GC], no. 28341/95, §§ 43-44, ECHR 2000-V).»

Det er med andre ord flere elementer som er relevante ved vurderingen av om behandling av offentlig tilgjengelige opplysninger utgjør et inngrep i privatlivet. Hvilke forventninger vedkommende har til personvern, kan i denne sammenheng være et viktig, men ikke nødvendigvis avgjørende, element. I *Rotaru mot Romania* 4. mai 2000, som gjaldt lagring av informasjon innhentet fra offentlig tilgjengelige kilder, viste domstolen til at offentlig tilgjengelig informasjon også kan falle inn under EMK artikkel 8 når det er snakk om mer systematisk innhenting og lagring i mapper oppbevart av myndighetene. Dette gjelder særlig dersom opplysningene omhandler forhold om en person som ligger langt tilbake i tid, se avsnitt 43.

At sikkerhetsmyndighetenes lagring av offentlig tilgjengelig informasjon som vedrører enkeltmenneskers privatliv kan utgjøre et inngrep i retten til respekt for privatlivet, følger også av *Leander mot Sverige* avsnitt 48 og *Segerstedt-Wiberg and Others mot Sverige* 6. september 2006 avsnitt 71 og 72. I sistnevnte avgjørelse sies det uttrykkelig at dette også gjaldt den delen av informasjonen som var offentlig tilgjengelig.

Praksis fra EMD viser etter dette at dersom innhentingen av informasjon er systematisk, informasjonen lagres over tid og utleveres til andre, vil behandlingen av opplysningene kunne være et inngrep i privatlivet etter EMK artikkel 8 nr. 1, selv om informasjonen er offentlig tilgjengelig.

5.1.2 Kort om masseinnsamling

EMD har også vurdert saker om masseinnhenting av informasjon, der innsamlingen som utgangspunkt ikke er systematisk eller rettet mot en konkret person. De aktuelle sakene dreier seg om hemmelig overvåking av kommunikasjon i transitt, der både innholdet i kommunikasjonen og metadata samles inn. Departementet er ikke kjent med praksis som gjelder masseinnhenting fra åpne kilder. Masseinnhenting fra åpne kilder skiller seg fra hemmelig overvåking av kommunikasjon i transitt og andre former for hemmelig overvåking av privat kommunikasjon. Som følge av dette har de kravene som er oppstilt i dommene nedenfor etter departementets vurdering begrenset overføringsverdi for forslaget i denne proposisjonen. Det gjøres likevel kort rede for enkelte dommer om masseovervåking av kommunikasjon i transitt.

EMDs nyeste avgjørelser om slik masseovervåking er avgjørelsene i storkammersakene *Big Brother Watch og andre mot Storbritannia* og *Centrum för Rättvisa mot Sverige,* begge fra 25. mai 2021. EMD la i disse avgjørelsene til grunn at masseinnsamling er en gradvis prosess, der omfanget av inngrepet i individets rettigheter etter artikkel 8 tiltar underveis, se *Big Brother Watch og andre mot Storbritannia* avsnitt 325 til 331. Selv på det første stadiet, der innhentingen og lagringen ikke er rettet mot konkrete individer, vil inngrepet rammes av EMK artikkel 8. Domstolen har i denne sammenheng vist til at også lagring av informasjon innebærer et inngrep i rettighetene etter EMK artikkel 8. Behovet for sikkerhetsmekanismer vil imidlertid være størst mot slutten av prosessen, når innholdet i kommunikasjonen blir nærmere undersøkt, se avsnitt 330.

I *Big Brother Watch og andre mot Storbritannia* avsnitt 360 og 361 oppstiller domstolen åtte kriterier som inngår i en helhetlig vurdering av om et regime for masseinnsamling er i samsvar med lovgivningen og nødvendig i et demokratisk samfunn:

> «360. In the light of the above, the Court will determine whether a bulk interception regime is Convention compliant by conducting a global assessment of the operation of the regime. Such assessment will focus primarily on whether the domestic legal framework contains sufficient guarantees against abuse, and

whether the process is subject to «end-to-end safeguards» (see paragraph 350 above). In doing so, it will have regard to the actual operation of the system of interception, including the checks and balances on the exercise of power, and the existence or absence of any evidence of actual abuse (see Association for European Integration and Human Rights and Ekimdzhiev, cited above, § 92).

361. In assessing whether the respondent State acted within its margin of appreciation (see paragraph 347 above), the Court would need to take account of a wider range of criteria than the six Weber safeguards. More specifically, in addressing jointly «in accordance with the law» and «necessity» as is the established approach in this area (see Roman Zakharov, cited above, § 236 and Kennedy, cited above, § 155), the Court will examine whether the domestic legal framework clearly defined:

1. the grounds on which bulk interception may be authorised;
2. the circumstances in which an individual's communications may be intercepted;
3. the procedure to be followed for granting authorisation;
4. the procedures to be followed for selecting, examining and using intercept material;
5. the precautions to be taken when communicating the material to other parties;
6. the limits on the duration of interception, the storage of intercept material and the circumstances in which such material must be erased and destroyed;
7. the procedures and modalities for supervision by an independent authority of compliance with the above safeguards and its powers to address non-compliance;
8. the procedures for independent ex post facto review of such compliance and the powers vested in the competent body in addressing instances of non-compliance.»

Masseinnsamling av kommunikasjonsopplysninger har også vært vurdert av EU-domstolen, blant annet i saken *La Quadrature du Net and Others* (sak C-511/18) fra 6. oktober 2020. Domstolen slo der fast at generell og udifferensiert innsamling og lagring av slike opplysninger ville være i strid med grunnleggende rettigheter og EUs kommunikasjonsverndirektiv. På visse vilkår er det imidlertid adgang til å ha regler om slik lagring ved en alvorlig trussel mot den nasjonale sikkerheten som må anses for å være reell og aktuell eller forutsebar, når dette tidsmessig er begrenset til det strengt nødvendige (som kan forlenges) og det foreligger tiltak som beskytter de berørtes kommunikasjonsopplysninger mot misbruk, jf. avgjørelsen avsnitt 137 og 138.

5.1.3 EMKs krav til lovhjemmel og proporsjonalitet ved inngrep i privatlivet

Inngrep i privatlivet kan være lovlig dersom vilkårene i EMK artikkel 8 nr. 2 er oppfylt. Her fremgår det at inngrepet må ha hjemmel i nasjonal lovgivning og være nødvendig i et demokratisk samfunn av hensyn til blant annet nasjonal sikkerhet eller forebygging av uorden eller kriminalitet.

I kravet om hjemmel i nasjonal lovgivning ligger at inngrepet må ha grunnlag i en formell nasjonal norm som er tilgjengelig og gir forutsigbarhet for innbyggerne. Om de kvalitative kravene som stilles til lovhjemmelen for inngrep, heter det i Rt. 2014 side 1105 avsnitt 30:

> «For å gi en slik hjemmel som Grunnloven og menneskerettskonvensjonene krever, holder det ikke at loven er formelt sett i orden, og at den etter alminnelige tolkningsprinsipper gir grunnlag for lagringen. Det gjelder også kvalitative krav: Loven må være tilgjengelig og så presis som forholdene tillater. Den må dessuten – i lys av den forhøyede risikoen for misbruk og vilkårlighet som erfaringsmessig kan foreligge når myndigheter tillates å operere i hemmelighet – gi rimelige garantier knyttet til blant annet formen for lagring, bruken av materialet, mulighetene for innsyn, sikkerhet og sletting.»

I *Rotaru mot Romania* avsnitt 56 uttales om lovskravet relatert særskilt til sikkerhetsmyndighetenes lagring og bruk av informasjon:

> «The quality of the legal rules relied on in this case must therefore be scrutinised, with a view, in particular, to ascertaining whether domestic law laid down with sufficient precision the circumstances in which the RIS could store and make use of information relating to the applicant's private life.»

Vilkåret om at inngrepet må være nødvendig i et demokratisk samfunn innebærer et krav om forholdsmessighet ved at behandlingen av informasjonen må være egnet til å oppnå det legitime formålet det skal ivareta. Legitime formål som kan begrunne inngrep i retten til privatliv er blant

annet hensynet til offentlig trygghet og hensynet til å forebygge uorden og kriminalitet.

Hvorvidt inngrepet er forholdsmessig må vurderes konkret. EMD har lagt til grunn at statene har en nokså vid skjønnsmargin ved vurderingen av hvilke tiltak som kan være egnet til å ivareta nasjonal sikkerhet. I kravet om at tiltaket skal være egnet til å oppnå formålet det er ment å ha, ligger at det må forventes å ha effekt. Det er videre et krav at formålet ikke kan ivaretas gjennom andre og mindre inngripende tiltak. Inngrepet må ikke være uunnværlig, men det må være et tvingende samfunnsmessig behov for det. I *Leander mot Sverige* avsnitt 58, heter det om denne vurderingen:

> «The notion of necessity implies that the interference corresponds to a pressing social need and, in particular, that it is proportionate to the legitimate aim pursued (…).»

Sentralt i vurderingen av forholdsmessigheten av systemer for hemmelig overvåking er hvorvidt det eksisterer tilstrekkelige og effektive garantier mot misbruk og vilkårlighet. Hvilke garantier som er nødvendige, må vurderes i lys av inngrepets art og omfang, se *P.G. og J.H. mot Storbritannia*, avsnitt 46.

Breyer mot Tyskland, 30. januar 2020, som gjaldt ekomtilbyderes plikt etter tysk telekommunikasjonslovgivning til å registrere informasjon som identifiserer kunder med forhåndsbetalte SIM-kort, kan også være av relevans. Domstolen tok der i sin proporsjonalitetsvurdering utgangspunkt i at kriminalitetsbekjempelse, særlig bekjempelse av organisert kriminalitet og terrorisme, samt ivaretakelse av offentlig sikkerhet og beskyttelse av borgere, utgjorde tvingende samfunnsmessige behov («pressing social needs»). I den forbindelse anerkjente domstolen at moderne kommunikasjonsformer og endrede kommunikasjonsvaner krever at etterforskingsverktøyene tilpasses, jf. avsnitt 88.

EMD så videre hen til hvor inngripende tiltaket var. Det ble lagt til grunn at *«the interference was, while not trivial, of a rather limited nature»*, jf. avsnitt 95. Ved vurderingen av nødvendige garantier mot misbruk mv., viste EMD blant annet til at lagringstiden ikke fremsto som for lang i lys av behovet, og at omfanget av lagrede data syntes å være begrenset til det som var nødvendig for formålet, jf. avsnitt 96. Det ble samtidig lagt til grunn at proporsjonalitetsvurderingen ikke bare kunne knytte seg til reglene for lagring, men også muligheten for tilgang til og bruk av opplysningene, jf. avsnitt 97. Ved vurderingen av tilgangsreglene viste EMD blant annet til at det var tilstrekkelig klart angitt hvilke myndigheter som kan kreve å få opplysningene utlevert, jf. avsnitt 99.

EMD har også innfortolket et krav om effektiv og uavhengig kontroll for å hindre myndighetsmisbruk, se blant annet *Rotaru mot Romania* avsnitt 59. Her fremgår det at kontrollen normalt bør ligge hos domstolene, i alle fall i siste instans, fordi *«judicial control affords the best guarantees of independence, impartiality and a proper procedure»*. EMD har imidlertid akseptert at andre enn domstolene kan oppfylle kravene til effektiv, uavhengig og permanent kontroll, se blant annet *Klass and others mot Tyskland,* 6. september 1978*,* som gjaldt lovligheten av regler om hemmelig overvåking av brev, post og telekommunikasjon, avsnitt 55 og 56. I *Breyer mot Tyskland* pekte EMD, under henvisning til sistnevnte sak, blant annet på at tidligere rettspraksis om mekanismer for kontroll med mer vesentlige inngrep i privatlivet, hadde begrenset overføringsverdi til saker der inngrepet var mindre. I avsnitt 103 er det uttalt:

> «In sum it considers that the level of review and supervision has to be considered as an important, but not decisive element in the proportionality assessment of the collection and storage of such a limited data set.»

Det var ikke et krav etter de tyske reglene at utlevering skulle godkjennes av en domstol eller av en annen uavhengig myndighet. EMD kom likevel til at mekanismene for tilsyn og kontroll var tilstrekkelige, og viste blant annet til datatilsynsmyndighetenes tilsynskompetanse og registrering av uttak av informasjon, se avsnitt 105 til 107.

Kravene etter Grunnloven § 102 og EMK artikkel 8 som er gjennomgått ovenfor setter rammer for utformingen av de reglene som departementet nå foreslår. Behandlingen må ha et rettslig grunnlag, regelen må være tilgjengelig og være utformet så vidt presist at borgerne kan forutberegne sin stilling. Videre må det foreligge sikkerhetsmekanismer som hindrer vilkårlighet og myndighetsmisbruk.

5.2 Ytringsfriheten – Grunnloven § 100 og EMK artikkel 10

Ytringsfriheten er vernet av både Grunnloven § 100, EMK artikkel 10 og SP artikkel 19. Ettersom Grunnloven § 100 og SP artikkel 19 ikke gir et mer omfattende vern av ytringsfriheten enn det

som følger av EMK artikkel 10, konsentreres fremstillingen om sistnevnte, som i norsk oversettelse lyder:

«1. Enhver har rett til ytringsfrihet. Denne rett skal omfatte frihet til å ha meninger og til å motta og meddele opplysninger og ideer uten inngrep av offentlig myndighet og uten hensyn til grenser. Denne artikkel skal ikke hindre stater fra å kreve lisensiering av kringkasting, fjernsyn eller kinoforetak.
2. Fordi utøvelsen av disse friheter medfører plikter og ansvar, kan den bli undergitt slike formregler, vilkår, innskrenkninger eller straffer som er foreskrevet ved lov og som er nødvendige i et demokratisk samfunn av hensyn til den nasjonale sikkerhet, territoriale integritet eller offentlige trygghet, for å forebygge uorden eller kriminalitet, for å beskytte helse eller moral, for å verne andres omdømme eller rettigheter, for å forebygge at fortrolige opplysninger blir røpet, eller for å bevare domstolenes autoritet og upartiskhet.»

Ytringsfriheten er ikke absolutt. Etter EMK artikkel 10 nr. 2 kan det gjøres inngrep i ytringsfriheten når det er foreskrevet ved lov og nødvendig i et demokratisk samfunn av hensyn til blant annet den nasjonale sikkerhet, territoriale integritet eller offentlige trygghet, og for å forebygge uorden eller kriminalitet. Kravet om at inngrepet må være foreskrevet ved lov, innebærer at det må ha grunnlag i nasjonal rett, at regelen må være tilgjengelig slik at den gir den enkelte tilfredsstillende angivelse av hvilke regler som gjelder i et konkret tilfelle, og at regelen er tilstrekkelig presist formulert til at den enkelte kan tilpasse sin atferd etter den. Vurderingskriteriet etter EMK artikkel 10 nr. 2 er blant annet oppsummert i HR-2021-526-A avsnitt 63 flg.

Kravet om at inngrepet må være nødvendig i et demokratisk samfunn, betyr etter praksis fra EMD blant annet at inngrepet må være egnet til å ivareta formålet med tiltaket, og at formålet ikke kan nås med mindre inngripende midler. Bestemmelsen gir anvisning på at det skal foretas en forholdsmessighetsvurdering, der de samfunnsmessige hensynene inngrepet skal ivareta, må veies mot konsekvensene av inngrepet for den enkelte som rammes.

Som nevnt i punkt 5.1.2 er departementet ikke kjent med rettspraksis som gjelder masseinnhenting av informasjon fra åpne kilder og forholdet til EMK artikkel 8. Departementet er heller ikke kjent med slike saker som gjelder forholdet til EMK artikkel 10. Retten til ytringsfrihet henger imidlertid ofte tett sammen med retten til privatliv, slik at et inngrep i retten til privatliv etter omstendighetene også vil kunne utgjøre et inngrep i ytringsfriheten. I *Segerstedt-Wiberg and Others mot Sverige,* avsnitt 105 til 107, kom EMD til at dersom behandlingen av informasjon om politisk aktivitet ikke kunne rettferdiggjøres etter EMK art 8 nr. 2, ville behandlingen også innebære et ulovlig inngrep i EMK artikkel 10 og 11 (forsamlings- og foreningsfriheten).

Selv om det ikke legges begrensninger på retten til å ytre seg, vil forslaget her kunne tenkes å ha en nedkjølende effekt på ytringsfriheten. Enkelte kan tenkes å ville modifisere eller sensurere ytringene sine, eller helt unnlate å ytre seg på internett, av frykt for eller kunnskap om at ytringene vil kunne lagres hos PST. Departementet legger derfor til grunn at forslaget etter omstendighetene vil kunne utgjøre et inngrep i ytringsfriheten.

5.3 Europarådets personvernkonvensjon

Norge har ratifisert Europarådets konvensjon nr. 108 av 28. januar 1981 om personvern i forbindelse med elektronisk databehandling av personopplysninger. Formålet med konvensjonen er å sikre respekten for individets rettigheter og grunnleggende friheter, særlig retten til privatliv, med hensyn til elektronisk databehandling av personopplysninger. Ved endringsprotokoll 10. oktober 2018 er det oppstilt mer detaljerte krav enn i gjeldende konvensjon. Endringsprotokollen har ikke trådt i kraft. Norge har signert endringsprotokollen og avgitt en erklæring om midlertidig anvendelse av protokollen.

Konvensjonens artikkel 9 nr. 2 åpner for at det kan gjøres unntak fra en rekke av konvensjonens krav når det følger av lov og er et nødvendig tiltak i et demokratisk samfunn av hensyn til blant annet beskyttelse av statens sikkerhet og offentlig sikkerhet og kriminalitetsbekjempelse. Det samme gjør endringsprotokollen artikkel 14. Det kan blant annet gjøres unntak fra en rekke av de alminnelige kravene for behandling av opplysninger etter artikkel 5 nr. 4, blant annet krav til at opplysninger skal behandles for de formål de er innhentet for, at det ikke skal behandles flere opplysninger enn nødvendig for formålet og at opplysningene skal være korrekte og oppdaterte. Det

kan også gjøres unntak fra reglene om informasjon til den registrerte og den registrertes rettigheter. For behandling av hensyn til nasjonal sikkerhet kan det gjøres ytterligere unntak.

Vurderingen av hvorvidt unntaket har hjemmel i lov, forfølger et legitimt formål og er nødvendig i et demokratisk samfunn er i hovedtrekk sammenfallende med vurderingstemaene som gjelder lovligheten av inngrep i rettighetene etter Grunnloven § 102 første ledd første punktum og EMK artikkel 8. Departementet legger derfor til grunn at tiltak som er forenlig med Grunnloven og EMK, heller ikke vil være i strid med Europarådskonvensjon nr. 108 om personvern i forbindelse med elektronisk databehandling av personopplysninger.

6 Andre lands rett

6.1 Danmark

Politiets Efterretningstjenestes (PET) oppdrag er angitt i den danske PET-loven § 1. Loven nevner ikke etterretningsvirksomhet som en egen oppgave eller et eget oppdrag for PET. PET skal blant annet forebygge, etterforske og motvirke brudd på den danske straffeloven kapittel 12 og 13, utarbeide trusselvurderinger og holde justisministeren underrettet om forhold av betydning for landets indre sikkerhet mv. Det fremgår av § 3 at PET kan samle inn og behandle opplysninger som kan ha betydning for tjenestens virksomhet.

PETs behandling av opplysninger er regulert i PET-loven kapittel 5 om intern behandling av personopplysninger. Direktiv (EU) 2016/680 er i Danmark gjennomført i lov om retshåndhævende myndigheders behandling af personoplysninger (retshåndhævelsesloven). Direktivet er ikke fullt ut gjort gjeldende for PET, men det er i PET-loven § 6 a angitt en del prinsipper for behandling av opplysninger, herunder krav om formålsbestemthet, krav til relevans og tilstrekkelighet, kvalitetskontroll og sletting.

I den danske politiloven ble det ved lov 8. juni 2017 tilføyd en ny § 2 a som bestemmer at politiet kan samle inn og behandle opplysninger fra offentlig tilgjengelige kilder når det er nødvendig av hensyn til utførelsen av politiets oppgaver. Bestemmelsen regulerer også sammenstillinger av opplysninger og tverrgående informasjonsanalyser. Det fremgår av forarbeidene til bestemmelsen at den ikke innebærer en utvidet adgang til å samle inn opplysninger fra åpne kilder, men at den sikrer et klart hjemmelsgrunnlag for politiets innsamling og behandling av – ofte betydelige mengder – opplysninger fra offentlig tilgjengelige kilder. Det er forutsatt i forarbeidene at det skal gis nærmere regler om behandlingen, herunder utlevering og sletting. Slike nærmere regler er foreløpig ikke gitt. Bestemmelsen gjelder kun for ordinært politi i Danmark.

6.2 Sverige

Säkerhetspolisens mandat er angitt i polislagen (1984:387) 3 §. Bestemmelsens første ledd lyder:

> «Till Säkerhetspolisens uppgifter hör att
> 1. förebygga, förhindra och upptäcka brottslig verksamhet som innefattar brott mot rikets säkerhet eller terrorbrott,
> 2. utreda och beivra sådana brott som anges i 1 eller som följer av 5,
> 3. fullgöra uppgifter i samband med personskydd av den centrala statsledningen och andra som regeringen eller Säkerhetspolisen bestämmer,
> 4. fullgöra uppgifter enligt säkerhetsskyddslagen (2018:585),
> 5. leda annan polisverksamhet om regeringen föreskriver det och i övrigt bedriva sådan verksamhet som framgår av lag eller förordning eller som regeringen uppdragit åt Säkerhetspolisen att i särskilda hänseenden ansvara för.»

Lag (2019:1182) om Säkerhetspolisens behandling av personuppgifter og förordning (2019:1235) om Säkerhetspolisens behandling av personuppgifter trådte i kraft 1. januar 2020. Loven gjennomfører til dels direktiv (EU) 2016/680 for Säkerhetspolisens del. Behandling av opplysninger fra åpne kilder er ikke regulert særskilt, verken for det alminnelige politi eller for Säkerhetspolisen. Innsamling av større mengder data som inneholder personopplysninger, må behandles i tråd med grunnkravene om at opplysningene må være nødvendig for et relevant formål innenfor tjenestens oppgaver. Innhenting av data fra åpne kilder, som ofte vil inneholde personopplysninger som tjenesten ikke er interessert i, vil derfor i mange tilfeller ikke være i tråd med disse grunnvilkårene.

6.3 Finland

Mandatet for Skyddspolisen (SUPO) fremgår av polisförvaltningslagen (14.2.1992/110) § 10. Bestemmelsens første ledd lyder:

> «Skyddspolisen har till uppgift att i enlighet med inrikesministeriets styrning inhämta information för att skydda den nationella säkerheten samt upptäcka, förhindra och avslöja sådan verksamhet, sådana förehavanden och sådana brott som kan hota statsskicket och samhällsordningen eller rikets inre eller yttre säkerhet. Skyddspolisen ska även upprätthålla och utveckla en allmän beredskap för att upptäcka och förhindra aktivitet som hotar samhällets säkerhet.»

Regler om behandling av personopplysninger fremgår av lag om behandling av personuppgifter i polisens verksamhet (10.5.2019/616) kapittel 7. Behandling av opplysninger fra åpne kilder er ikke særskilt regulert. Informasjon fra åpne kilder kan innhentes og brukes dersom tjenesten kan vise til et behov for informasjonen som ligger innenfor tjenestens lovpålagte oppgaver. I medhold av lag om behandling av personuppgifter i polisens verksamhet, kan lagring av personopplysninger som er innhentet fra åpne kilder bare skje når opplysningene er relevante for tjenestens oppgaveløsning.

I 2019 vedtok Finland lovendringer om sivil etterretningsvirksomhet, se lag om civil underrättelsesinhämtning avseende datatrafikk (26.4.2019/582) og nytt kapittel 5 a i polislagen (22.7.2011/872). Lovendringene innebar en styrking av SUPOs mandat til å drive sivil etterretningsvirksomhet, og ga tjenesten hjemmel for å drive informasjonsinnhenting med det formål å sikre nasjonale sikkerhetsinteresser og støtte beslutningstakingen i den øverste statsledelsen, jf. polislagen 5 a kap § 1. Lovendringen utvidet tjenestens mandat til å drive etterretningsvirksomhet utover der formålet for innhentingen er å avdekke, forebygge og etterforske straffbar virksomhet.

I tillegg ble SUPOs mandat utvidet slik at tjenesten også kan drive etterretningsvirksomhet i utlandet når formålet er å sikre Finlands nasjonale sikkerhet, samt at det ble åpnet for at SUPO kunne drive innhenting av grenseoverskridende datatrafikk, jf. lag om civil underrättelseinhämtning avseende datatrafik (26.4.2019/582).

6.4 Andre land

De fleste land utenfor Norden har rene innenlands etterretnings- og/eller sikkerhetstjenester som ikke har noen rolle som politiorgan. I flere vestlige land har landenes innenlands sikkerhetstjenester også i oppgave å drive med innenlands etterretning knyttet til trusler i henhold til tjenestenes respektive mandater. Eksempler på slike tjenester er Secret Service/MI5 (Storbritannia), Bundesamt für Verfassungsschutz/BfV (Tyskland), Federal Bureau of Investigation/FBI (USA) og Algemene Inlichtingen- en Veiligheidsdienst/General Intelligence and Security Service (Nederland).

7 Regulering av PSTs etterretningsoppdrag

7.1 Forslaget i høringsnotatet

I høringsnotatet ble det vist til at selv om PST har rollen som Norges innenlands etterretningstjeneste, og det en rekke steder er forutsatt at PST skal drive etterretning innenfor sitt mandat, fremgår ikke dette direkte av politiloven.

Som følge av at nødvendighetskravet i politiregisterloven § 64 er knyttet til PSTs oppgaver etter politiloven, kan PST derfor heller ikke uten videre behandle opplysninger kun for dette formålet. PST har i dag begrensede muligheter til å jobbe med enkelte typer trusler fordi de ikke er belagt med straff, herunder for eksempel kartlegging av radikalisering og ekstreme subkulturer innen digitale nettverk, avdekking av statlig styrte påvirkningskampanjer og fremmede staters oppkjøp av samfunnskritisk infrastruktur. PSTs vurderinger av fremtidig trusselutvikling baseres i dag primært på informasjon som er innhentet til andre formål, noe som gjør at vurderingene kan være basert på et utilstrekkelig etterretningsgrunnlag og medføre fare for etterretningssvikt.

På bakgrunn av dette ble det foreslått endringer i politiloven § 17 a slik at det fremgår eksplisitt at PST, i tillegg til et politiorgan, også er Norges nasjonale innenlands etterretningstjeneste. Det ble vist til at endringen ikke i seg selv innebærer realitetsendringer.

Som følge av at «etterretning» ikke er et entydig rettslig begrep med et klart innhold, og kan benyttes både om en arbeidsprosess, et produkt som kommer ut av prosessen og om organisasjonen som utøver etterretning, mente departementet at det burde gis en mer konkret beskrivelse av hva oppgaven som innenlands etterretningstjeneste innebærer.

Det ble derfor foreslått et nytt ledd i politiloven § 17 b om at PST skal drive etterretningsvirksomhet i tilknytning til de straffbare forhold som PST skal forebygge og etterforske samt for utarbeidelse av trusselvurderinger, herunder kartlegge trender og utviklingstrekk som har tilknytning til dette formålet, og i denne forbindelse utarbeide analyser og etterretningsvurderinger. Endringen var ment å klargjøre formålet med den delen av tjenestens virksomhet som skjer i forkant av det straffbare, og som går ut over det som naturlig kan betegnes som forebygging.

Høringsnotatet fremholdt også behovet for å tydeliggjøre PSTs etterretningsoppdrag i forbindelse med utarbeidelse av trusselvurderinger og åpne for at PSTs trusselvurderinger kan baseres på et bredere informasjonstilfang enn i dag. Slike vurderinger kan eksempelvis omfatte kartlegging og vurdering av påvirkningsvirksomhet, oppkjøp fra utenlandske aktører, kartlegging av forhold som kan medføre fare for radikalisering eller avdekking av nye og hittil ukjente trusler samfunnet står ovenfor i fremtiden.

Endringen var ment å synliggjøre at PST også skal drive strategisk og kunnskapsbasert etterretning innenfor tjenestens ansvarsområde, der formålet er å gi et overordnet bilde av fenomener, trender og utvikling av trusselrelatert aktivitet i Norge, og derigjennom gi god beslutningsstøtte.

Som følge av lovreguleringen av PSTs etterretningsoppdrag ble det foreslått å tilføye et nytt nr. 6 i politiregisterloven § 64 tredje ledd om at PST kan behandle opplysninger når det er nødvendig for etterretningsvirksomheten.

7.2 Høringsinstansenes syn

Forsvarsdepartementet, Politiets sikkerhetstjeneste (PST), Finnmark politidistrikt, Kripos, Politidirektoratet, Riksadvokaten, Direktoratet for samfunnssikkerhet og beredskap (DSB), Datatilsynet, Norges institusjon for menneskerettigheter (NIM), Advokatforeningen og *UTSYN* har uttalt seg om forslaget om å lovfeste PSTs etterretningsoppdrag og gi en hjemmel for å behandle opplysninger for dette formålet. Høringsinstansene støtter i all hovedsak intensjonen bak forslaget, men flere har merknader til hvordan oppdraget er foreslått formulert.

Forsvarsdepartementet støtter intensjonen bak å tydeliggjøre PSTs etterretningsoppdrag i lov, nemlig å utvide behandlingsgrunnlaget for opplysninger som ikke er koblet direkte til en pågående sak, men som likevel har betydning for PSTs evne til å løse sitt lovpålagte oppdrag. PST bør ha

mulighet til å kartlegge trender og utviklingstrekk på egnet måte. Forslaget om å regulere dette som en oppgave i politiloven skaper imidlertid etter Forsvarsdepartementets syn noen prinsipielle uklarheter.

Forsvarsdepartementet støtter at det presiseres i § 17 a at PST er Norges innenlands etterretnings- og sikkerhetstjeneste. Ettersom PST er en del av politiet og utøver etterretningsvirksomheten med et politimessig formål, er det misvisende å si at rollen som innenlands etterretningstjeneste utøves «i tillegg til» å være et politiorgan. Etterretningsfunksjonen er direkte knyttet til sikkerhetsfunksjonen, og det lar seg ikke gjøre å trekke et skarpt skille mellom disse.

Forsvarsdepartementet stiller spørsmål om det er behov for forslaget om PSTs etterretningsvirksomhet i nytt fjerde ledd i politiloven § 17 b. Alternativt må forslaget til regulering etter deres syn formuleres tydeligere, ettersom etterretning er en systematisk måte å innhente og behandle informasjon på, og ikke en selvstendig oppgave. Dersom PST skal gis anledning til mer generell kartlegging av aktivitet i Norge, inklusive av lovlige handlinger som lovlig påvirkningsvirksomhet og fremmede staters oppkjøp av samfunnskritisk infrastruktur, vil dette være en prinsipiell utvidelse av PSTs myndighet som må begrunnes nærmere. Også rammene for dette og hvilke virkemidler som kan tas i bruk må beskrives og begrunnes nærmere.

Forsvarsdepartementet savner videre en vurdering av om en eventuell oppdatering av behandlingsgrunnlaget i politiregisterloven § 64 kunne vært en mer hensiktsmessig løsning på de problemstillinger som skisseres. Slik de leser bestemmelsen åpner blant annet tredje ledd nr. 2 for behandling av opplysninger utenfor en konkret sak når dette er nødvendig for tjenestens utarbeidelse av trusselvurderinger. Dersom bestemmelsen ikke i tilstrekkelig grad hjemler behandling av opplysninger for å kunne si noe om trender og utviklingstrekk i forbindelse med trusselvurderinger, kan dette eventuelt presiseres nærmere i bestemmelsen.

Etter politiregisterloven § 64 første ledd kan PST bare behandle opplysninger når det er nødvendig ut fra politimessige formål eller forvaltningsvirksomheten i tjenesten, noe som ikke er foreslått endret. Forsvarsdepartementet støtter dette. Behandlingen med innenlands etterretningsformål som PST gjør i dag og som foreslås presisert i lov, skjer med et politimessig formål all den tid virksomheten må kobles opp mot et konkret straffbart forhold eller utviklingstrekk av ulovlig aktivitet som PST skal forebygge eller etterforske.

PST mener det er behov for å tydeliggjøre PSTs etterretningsoppdrag slik at tjenesten gis mulighet til å innhente opplysninger for dette formålet. Gjennom etterretningsinformasjon dannes grunnlag for tidsriktige og brede trusselvurderinger og analyser.

Etter politiregisterloven er PSTs anledning til å behandle opplysninger begrenset til behandling med sikte på kriminalitetsbekjempelse i konkrete tilfeller. Konsekvensen av dette er at når PST ved utarbeidelsen av analyser, trusselvurderinger eller annen beslutningsstøtte skal si noe om den generelle sikkerhetstrusselen mot Norge, bygger dette på informasjon som er innhentet i konkrete enkeltsaker. Dette er historisk informasjon på kontraterror- og kontraetterretningssiden, med kriminalitetsbekjempelse som formål. Denne informasjonen generaliseres så for å søke å gi et bredere bilde.

Ettersom PST i dag ikke har et tydelig etterretningsmandat eller grunnlag for å innhente og behandle opplysninger knyttet til et slikt oppdrag, risikerer norske myndigheter etterretningssvikt. Etterretningssvikt kan for eksempel være presentasjon av uriktig eller mangelfull informasjon som beslutningsstøtte. For å unngå etterretningssvikt er det viktig at PSTs oppdrag som Norges innenlandske etterretningstjeneste klargjøres, og at det etableres nødvendig hjemmel for innhenting av opplysninger for dette formålet. I tillegg til et klarere mandat for PSTs etterretningsvirksomhet vil det være nødvendig med forutsigbare og klare hjemler i behandlingsregelverket som muliggjør behandling av opplysninger for denne delen av tjenestens arbeid.

Riksadvokaten er i utgangspunktet positiv til at PSTs oppgaver tydeliggjøres i loven, og fremhever betydningen av at PSTs mandat er klarest mulig. Dette har en side til ansvarslinjene og det tosporede system, og er viktig for å sikre at PST ikke utøver myndighet utover lovgivers forutsetninger. Et sentralt aspekt ved sistnevnte er EOS-utvalgets kontrollmuligheter.

Riksadvokaten peker på at også politiet for øvrig driver etterretningsvirksomhet og utarbeider overordnede trusselvurderinger mv. Det kunne derfor være hensiktsmessig dersom departementet i det videre arbeidet også omtaler hvordan overveielsene relatert til PST forholder seg til det øvrige politiets virksomhet.

Etter Riksadvokatens oppfatning er det ikke nødvendigvis treffende å anse etterretning som et formål i seg selv, idet etterretning må anses mer

som en arbeidsmetode enn et selvstendig formål. Metoden brukes i ulike sammenhenger og med ulike formål, herunder både som ledd i forebygging og etterforsking. Regelverket kunne blitt tydeligere dersom det sondres klarere mellom formål og arbeidsmetode, og de ulike etterretningsformålene uttrykkelig og uttømmende angis i loven.

Riksadvokaten understreker at etterretning der siktemålet er å kartlegge om et straffbart forhold finner eller har funnet sted, og i tilfelle hvor, når og hvem som er ansvarlig, uansett vil være å anse som etterforsking og dermed høre under påtalemyndigheten. Riksadvokaten legger til grunn at forslaget ikke tar sikte på å endre dette. Slik bestemmelsen er utformet vil imidlertid også etterretningsvirksomhet som ledd i etterforsking være omfattet. Etterretningsbegrepet bidrar ikke nødvendigvis til klarhet om den viktige sondringen mellom etterforsking og annen virksomhet. Som følge av den løsning som er valgt kan det også oppstå spørsmål om forholdet til reglene i politiregisterloven.

Politidirektoratet, Det nasjonale statsadvokatembetet, Finnmark politidistrikt og *Kripos* støtter forslaget om å tydeliggjøre PSTs etterretningsoppdrag ved endringer i politiloven §§ 17 a og 17 b.

Når det gjelder endringene i § 17 a, stiller *Kripos* og *Politidirektoratet* spørsmål ved om oppdraget som innenlands etterretningstjeneste skal forstås å komme i tillegg til oppgaven som politiorgan. Etter deres vurdering er det mer treffende å se etterretningsoppdraget som en integrert del av den øvrige virksomheten. Politidirektoratet mener det også bør vurderes presisert i § 17 a at PST er landets innenlands «sikkerhetstjeneste».

Kripos og *Politidirektoratet* viser til at også politiet for øvrig møter en økende forventning om å bidra med beslutningsstøtte om kriminalitetsutvikling og andre forhold som går utover hva som tradisjonelt er omtalt som kriminaletterretning. Etterretning er i politiets etterretningsdoktrine ikke angitt som et eget formål, men utgjør en metode for behandling av opplysninger til politimessige formål. Det er mulig å se på etterretning både som et selvstendig formål, og som en metode som er egnet til å oppnå et annet politimessig formål. For politiet er det avgjørende at de foreslåtte lovendringene ikke medfører en endring i dette utgangspunktet.

Politidirektoratet oppfatter at formålet med den foreslåtte reguleringen er å gi PST et utvidet behandlingsgrunnlag knyttet til etterretningsvirksomhet – ut over det som kan knyttes til konkrete saker. De stiller spørsmål om det i stedet for å regulere etterretningsvirksomhet som en egen oppgave, ville være mer hensiktsmessig å gi et utvidet behandlingsgrunnlag i politiregisterloven § 64 for å kartlegge trender og utviklingstrekk som har tilknytning til ulovlig virksomhet innenfor PSTs ansvarsområde, for eksempel i tredje ledd nr. 2 om utarbeidelse av trusselvurderinger.

Datatilsynet mener at forslaget, kombinert med forslaget om bruk av åpent tilgjengelig informasjon, endrer PSTs rolle i en slik grad at det vil få konkrete konsekvenser for personvernet, samt at det bidrar til å gjøre rollefordelingen mellom de ulike etterretnings- og polititjenestene mer uklar. Det gjør kontroll vanskeligere, og kan føre til usikkerhet om i hvor stort omfang norske borgere blir utsatt for overvåking, noe som i seg selv kan bidra til nedkjølingseffekten.

NIM støtter at PSTs rolle og oppgaver klargjøres, men etterlyser en grundigere gjennomgang av de menneskerettslige effektene en slik utvidelse av PSTs overvåking i Norge kan føre med seg, særlig knyttet til retten til privatliv, personvern og retten til ytringsfrihet.

Advokatforeningen anerkjenner at den digitale hverdagen gir et stadig mer sammensatt og komplekst trusselbilde, og at den teknologiske og samfunnsmessige utviklingen bidrar til en betydelig økt informasjonsmengde. Som følge av dette er det et sterkt behov for rettidig, relevant og pålitelig etterretning som kan danne grunnlag for beslutninger av betydning for nasjonale sikkerhetsinteresser. Det synes klart at hovedformålet med lovforslaget er å sikre at PST får tilgang til et bredere informasjonsgrunnlag som trusselvurderingene og andre analyser kan baseres på. Advokatforeningen savner en grundigere redegjørelse for og drøftelse av hvorfor eksisterende hjemler og virkemidler ikke er tilstrekkelige for å oppnå det angitte formålet. Advokatforeningen mener at grensen mellom PSTs oppdrag knyttet til å følge med på utviklingen og individspesifikk etterretning ikke synes tilstrekkelig belyst.

UTSYN mener det er nødvendig at PST som etterretningstjeneste settes i stand til å utføre sitt lovpålagte samfunnsoppdrag på en adekvat måte, og er positiv til lovhjemler som setter sikkerhets- og etterretningstjenestene bedre i stand til å utføre sine lovpålagte oppgaver.

7.3 Departementets vurderinger

7.3.1 PSTs oppgaver som innenlands etterretningstjeneste

Departementet har merket seg at høringsinstansene som direkte har uttalt seg om forslaget til endringer i politiloven § 17 a, støtter det. Departementet opprettholder at det bør lovfestes i politiloven at PST er Norges innenlands etterretningstjeneste. Bestemmelsen foreslås imidlertid utformet på en annen måte enn i høringsnotatet.

Enkelte høringsinstanser har stilt spørsmål ved om det er et reelt behov for å en egen regulering av etterretningsoppdraget, eller om det er tilstrekkelig med en endring i politiregisterloven § 64 om nødvendighetskravet, eksempelvis ved en endring i tredje ledd nr. 2 om at opplysninger utenfor straffesak kan behandles der det er nødvendig for tjenestens utarbeidelse av trusselvurderinger.

Bestemmelsen i politiregisterloven § 64 tredje ledd nr. 2 korresponderer med den sentrale enhet (DSE) i PST sin oppgave i politiloven § 17 c nr. 1 om utarbeidelse av trusselvurderinger til bruk for politiske myndigheter. I Ot.prp. nr. 29 (2000–2001) Om lov om endringer i politiloven (overvåkingstjenestens oppgaver mv.), punkt 8.1 side 47 til 48, er politiloven § 17 c nr. 1 i stor grad omtalt som en bestemmelse om de periodiske trusselvurderingene PST skal utarbeide innenfor tjenestens områder og som fremlegges for politiske myndigheter. Vurderingene skal, heter det, danne grunnlag for overordnede rammebetingelser og prioriteringer for kommende år. I tillegg til slike overordnede trusselvurderinger utarbeider tjenesten mer spesifikke trusselvurderinger knyttet til konkrete hendelser, innenfor et samfunnsområde eller knyttet til enkeltpersoner.

Disse vurderingene beskriver imidlertid i begrenset grad for eksempel trender, utvikling eller fenomener som på lengre sikt kan true nasjonale sikkerhetsinteresser. Det oppgaven med utarbeidelse av trusselvurderinger er forstått å skulle omfatte, dekker ikke i seg selv behovet for å stadfeste PSTs mandat som innenlands etterretningstjeneste.

Som PST har vist til i sin høringsuttalelse, utarbeider tjenesten i dag trusselvurderinger basert på informasjon innhentet i konkrete saker, som søkes generalisert for å gi et bredere og mer overordnet bilde av en fremtidig trusselsituasjon. Så lenge tjenestens mandat er angitt som å forebygge og etterforske konkrete straffbare handlinger, vil ikke det at PST skal utarbeide trusselvurderinger i seg selv være en tilstrekkelig hjemmel for å kunne behandle opplysninger som er nødvendige for å utarbeide generelle, overordnede vurderinger som grunnlag for beslutningsstøtte. Som vist til i høringsnotatet vil utarbeidelse av slike vurderinger ikke nødvendigvis kunne betegnes som forebygging, og informasjon uten tilknytning til konkrete saker vil også være av betydning for å lage slike vurderinger. Departementet mener derfor at etterretningsoppdraget bør etableres som en egen oppgave i politiloven, fremfor å utvide de eksisterende behandlingshjemlene i politiregisterloven § 64.

Departementet er enig med de høringsinstansene som fremholder at etterretning i seg selv ikke er et selvstendig formål. Etterretning skjer for å oppnå noe, og ikke for sin egen del. Som det ble vist til i høringsnotatet er hensikten at PST skal kunne utarbeide vurderinger og analyser på et bredere grunnlag enn i dag, og uten at opplysningene som ligger til grunn for analysene må stamme fra en konkret sak. Departementet ser imidlertid at det kan fremstå som uklart hva forslaget innebærer når man knytter etterretningsvirksomheten til eksisterende oppgaver i politiloven.

Basert på høringsinnspillene fra bl.a. Riksadvokaten og Politidirektoratet, vurderer departementet at det er grunn til å skille tydeligere mellom kriminaletterretning som skjer for eksisterende politimessige formål, og som også de øvrige delene av politiet utfører, og oppgaven PST skal utføre etter den nye bestemmelsen. Forslaget her berører ikke kriminaletterretning som har til formål å kartlegge om et straffbart forhold finner eller har funnet sted, og som er en del av etterforskingen som faller inn under Riksadvokatens ansvarsområde. Ei heller griper det inn i kriminaletterretning i forebyggende øyemed, som også politiet for øvrig driver med. Slik forslaget var formulert kunne det imidlertid skape visse uklarheter på disse punktene.

Departementet mener derfor at det er behov for å tydeliggjøre og omformulere forslaget sammenlignet med det som ble sendt på høring, ettersom formuleringen om at etterretning skal drives i tilknytning til eksisterende oppgaver, ikke nødvendigvis er egnet til å skape tilstrekkelig klarhet. Fremfor å knytte analyser og etterretningsvurderinger til de områder som er dekket av politiloven § 17 b første ledd og utarbeidelse av trusselvurderinger, bør beskrivelsen av etterretningsoppdraget i større grad stå på egne ben. I oppgaven som innenlands etterretningstjeneste ligger det noe mer og til dels noe annet enn de oppgavene som

PST i dag har som politiorgan, noe som bør synliggjøres i lovteksten. Det er imidlertid nær sammenheng mellom oppgavene, ettersom de straffebudene som er listet opp i politiloven § 17 b i stor grad retter seg mot handlinger som også kan betegnes som trusler mot nasjonale sikkerhetsinteresser. Dette gjelder eksempelvis terrorlovbrudd, ulovlig etterretningsvirksomhet og spredning av masseødeleggelsesvåpen.

Det foreslås etter dette å regulere oppgaven som innenlands etterretningstjeneste i en egen bestemmelse hvor det fremgår at PST skal utarbeide analyser og etterretningsvurderinger om forhold i Norge som kan true Norges suverenitet, territorielle integritet, demokratiske styreform og andre nasjonale sikkerhetsinteresser. Det vises til forslaget til endret § 17 a om PSTs oppgave som innenlands etterretningstjeneste. Begrepet nasjonale sikkerhetsinteresser benyttes både i etterretningstjenesteloven og i sikkerhetsloven, og skal forstås på samme måte som etter definisjonen i sikkerhetsloven § 1-5 nr. 1. Dette vil også omfatte forhold som ikke nødvendigvis vil rammes av konkrete straffebestemmelser, men som på sikt kan true disse interessene. Som eksempler kan nevnes påvirkningsvirksomhet, oppkjøp fra utenlandske aktører eller økt omfang av eller endret utvikling knyttet til radikalisering. Det kan også omfatte forhold som ikke enda truer nasjonale sikkerhetsinteresser, men der man søker å avdekke aktivitet eller fenomener som på sikt kan true disse interessene. Bestemmelsen avgrenses mot de forhold som hører under E-tjenestens ansvarsområde, ved at analysene og etterretningsvurderingene skal gjelde forhold *i Norge*. Bestemmelsen vil erstatte den gjeldende politiloven § 17 a, hvis innhold i praksis dekkes av bestemmelsene i §§ 17 b og 17 c.

Analysene og vurderingene må videre knyttes til konkrete etterretningsbehov. I dette ligger at det må foreligge behov for informasjon om fremtidige eller eksisterende forhold som kan true nasjonale sikkerhetsinteresser. Behovet kan være definert av overordnet myndighet, fra en samfunnssektor eller egetinitiert av PST. Analysene og etterretningsvurderingene vil være rådgivende og er ment som beslutningsstøtte for å prioritere innsatsområder, ressurser og tiltak.

Forsvarsdepartementet uttaler i sitt høringssvar at det er uklart om det åpnes for at PST kan behandle informasjon uavhengig av om handlingen er lovlig eller ikke. Som nevnt innebærer forslaget at PST skal gi beslutningsstøtte om forhold i Norge som kan true nasjonale sikkerhetsinteresser, uten at vurderingen på aktuelt tidspunkt er knyttet til forebyggingen eller etterforskingen av et konkret straffbart forhold. Dette gjør at PST vil få anledning til å registrere opplysninger om lovlig virksomhet, så fremt opplysningene er nødvendige for utarbeidelse av analyser og etterretningsvurderinger. Kombinasjonen av ulike virkemidler, sivile og militære, åpne og fordekte, i det fysiske så vel som i det digitale rommet, medfører at trusselbildet er utfordrende og sammensatt. Dersom PST skal være i stand til å identifisere og avdekke om de virkemidlene som benyttes kan utgjøre en trussel mot nasjonale sikkerhetsinteresser, må tjenesten ha anledning til å behandle opplysninger om slike forhold.

Et konkret eksempel er sikkerhetstruende økonomisk virksomhet i Norge fra fremmede stater. Her vil norske myndigheter ha behov for kunnskap om omfanget og modus for slik aktivitet, som på sikt kan true nasjonale sikkerhetsinteresser. Etter dagens regelverk har PST begrensede muligheter til å arbeide med denne problemstillingen, ettersom tjenesten bare kan behandle opplysninger om forholdene dersom det foreligger indikasjoner på brudd på eksportkontrollregelverket eller indikasjoner på at andres staters etterretningstjenester er involvert i aktiviteten. I mange tilfeller er det behov for å behandle opplysninger i et videre omfang enn dette, for å gi beslutningsstøtte om trusselbildet.

Også dersom PST skal gi beslutningsstøtte om radikaliseringsprosesser eller gi et situasjonsbilde av omfanget av ulike ekstreme miljøer i Norge, må tjenesten kunne behandle opplysninger i større omfang enn i dag. For å kunne forebygge nye trusler fra radikale og ytterliggående miljøer må tjenesten vite hvordan slike miljøer utvikler seg. Tjenesten må også ha kunnskap om hvordan ekstremistiske personer og miljøer jobber for å skape aksept for bruk av vold overfor radikale og ytterliggående miljøer som opprinnelig ikke støtter bruk av vold, slik at disse miljøene på sikt kan utgjøre en trussel mot nasjonal sikkerhet.

Etter departementets vurdering vil en tydeliggjøring av etterretningsoppdraget for PST også styrke samarbeidet med E-tjenesten, og dermed bidra til å gi adekvat beslutningstøtte samlet sett til norske myndigheter om forhold som har betydning for nasjonale sikkerhetsinteresser. Dersom PST skal kunne behandle informasjon fra E-tjenesten og komplementere denne med informasjon om nasjonale forhold, må tjenestene ha tilsvarende muligheter til å behandle opplysninger. Videre kan det oppstå etterretningshull om forhold som kan utgjøre en trussel mot nasjonale sik-

kerhetsinteresser dersom ingen av tjenestene er gitt mandat til å arbeide med disse forholdene.

Departementet understreker at forslaget ikke innebærer at PST gis hjemmel til å bruke skjulte tvangsmidler for etterretningsformål. Adgangen til å bruke tvangsmidler utenfor etterforsking er uttømmende regulert i politiloven § 17 d, som ikke foreslås endret. PST får derved ingen utvidete virkemidler for å ivareta oppgaven, ut over at det kan behandles opplysninger som er nødvendige kun for dette formålet. Det vises imidlertid til forslaget om behandling av åpent tilgjengelig informasjon i punkt 8 nedenfor.

7.3.2 Hjemmel for behandling av opplysninger for etterretningsformål

Politiregisterloven § 64 gir særregler for PST om kravet til nødvendighet som vilkår å behandle opplysninger. Bakgrunnen for reglene er at PSTs oppgaver skiller seg fra det øvrige politiets virksomhet, ved at PSTs viktigste oppgave er å forebygge straffbare handlinger som kan true rikets sikkerhet. PST har derfor mulighet til å behandle opplysninger om en større personkrets enn hva som er tilfelle for politiet for øvrig. For å ivareta personvernet er adgangen til å behandle opplysninger knyttet til PSTs ulike oppgaver, samtidig som det er oppstilt vilkår som må være oppfylt for at behandlingen kan finne sted for den enkelte oppgaven.

Forslaget til endringer i § 64 tredje ledd nytt nr. 6 er derfor en følge av forslaget til endringer i PSTs oppgaver, jf. punktet over. Ordlyden er tilpasset formuleringen i forslaget til endringer i politiloven § 17 a, ved at det fremgår at PST kan behandle opplysninger som er nødvendig for å utarbeide analyser og etterretningsvurderinger som nevnt i denne bestemmelsen. Dette innebærer at PST vil kunne behandle opplysninger i et noe større omfang enn det tjenesten gjør i dag.

Skal det eksempelvis utarbeides analyser og vurderinger om omfanget av og utviklingen i fremmede staters oppkjøp av samfunnskritisk infrastruktur, kan tjenesten ha behov for å behandle opplysninger om personer som del av kartleggingen. Det samme gjelder ved undersøkelser av omfanget av ekstreme subkulturer innen digitale nettverk. Dersom PST skal evne å gi relevant beslutningsstøtte om fremmede staters bruk av sammensatte virkemidler som samlet kan utgjøre en trussel mot nasjonale sikkerhetsinteresser, må tjenesten ha mulighet til å behandle opplysninger om forhold som hver for seg ikke nødvendigvis kan relateres til straffbare forhold. Vurderingene vil være overordnede og gi et bilde av et fenomen eller en utvikling som kan utgjøre en trussel på sikt.

Opplysningene vil i denne sammenheng i utgangspunktet ikke være av interesse på individnivå, og skiller seg dermed fra de opplysningene PST behandler som ledd i en forebyggende sak eller etterforskingssak eller som ledd i en av sine andre lovpålagte oppgaver. I likhet med de andre oppgavene i politiregisterloven § 64 må imidlertid de øvrige vilkårene i loven være oppfylt, herunder kravene til opplysningenes kvalitet i § 6 og regelen om behandling av særlige kategorier av personopplysninger i § 7. I tillegg vil den alminnelige slettebestemmelsen i § 50 komme til anvendelse. Opplysningene må følgelig være korrekte, relevante og oppdaterte, og de skal slettes når de ikke lenger er nødvendige for formålet. Dette fordrer god notoritet for begrunnelser for registrering av opplysninger for etterretningsformål og kontroll med disse registreringene.

Forsvarsdepartementet har påpekt at § 64 første ledd om at PST bare kan behandle opplysninger når det er nødvendig ut fra politimessige formål og forvaltningsvirksomhet i tjenesten, ikke er foreslått endret. Dette gjør det etter Forsvarsdepartementets syn tydelig at bestemmelsen er ment å være begrenset til etterretning innenfor de politimessige formålene.

Departementet er enig i at utformingen av etterretningsoppdraget som foreslås i denne proposisjonen, til en viss grad avviker fra det som regnes som politiets kriminalitetsbekjempende virksomhet slik denne er definert i politiregisterloven § 2 nr. 13. Samtidig er politiregisterloven ment å regulere hele PSTs virksomhet. Departementet foreslår derfor at dette reflekteres i politiregisterloven § 3 om virkeområdet for loven, slik at det klart fremkommer at PSTs etterretningsvirksomhet er omfattet av loven. Det foreslås tilsvarende endring i § 64 første ledd, slik at det der fremgår at PST kan behandle opplysninger når det er nødvendig for politimessige formål, etterretningsvirksomhet og forvaltningsvirksomhet i tjenesten.

8 Behandling av åpent tilgjengelig informasjon

8.1 Overordnet om forslaget og de menneskerettslige rammene

8.1.1 Forslaget i høringsnotatet

I høringsnotatet ble det foreslått en ny § 65 a i politiregisterloven som åpner for at PST kan behandle åpent tilgjengelig informasjon for etterretningsformål, uten at politiregisterloven § 6 om krav til opplysningenes kvalitet og § 7 om behandling av særlige kategorier av personopplysninger kommer til anvendelse. Informasjon regnes ikke som åpent tilgjengelig dersom tilgang til informasjonen krever forsering av passord eller andre lignende beskyttelsesmekanismer. Som følge av at forslaget åpner for behandling av svært store mengder informasjon, anså departementet det viktig å begrense de mulige negative konsekvensene i størst mulig grad. Det ble derfor foreslått at opplysningene skal sperres, slik at de kun kan brukes til konkret angitte formål, og ellers ikke anses å være registrert hos PST. I tillegg til bruk for etterretningsformål mente departementet at opplysningene også burde kunne brukes til opprettelse av eller bruk i forebyggende sak og til etterforsking av lovbrudd innenfor PSTs ansvarsområde. Det ble foreslått at opplysningene skulle slettes senest etter 15 år, en frist som tilsvarte slettefristen i etterretningstjenesteloven § 9-8 for rådata innhentet i bulk.

I politiregisterforskriften ble det foreslått en forskriftsbestemmelse om at opplysninger som behandles etter den nye bestemmelsen skal holdes atskilt, og at tilgang kun skal gis til personer som har fått særskilt bemyndigelse. Det ble foreslått at bruk av opplysningene skal registreres og kunne spores for å kunne kontrollere om søkene og bruken er tillatt eller ikke. Registreringene skal gjennomgås regelmessig med det formål å avdekke uautorisert tilgang til opplysningene. I tillegg ble det foreslått at behandling av opplysningene for etterretningsformål kan skje ved bruk av automatiserte analyseverktøy. Det ble understreket at bruk av automatiserte analyseverktøy ikke kan skje med det formål å kartlegge enkeltindividers aktivitet på nett.

I høringsnotatet ble det vist til at forslaget vil innebære behandling av en slik art at det vil utgjøre et inngrep i privatlivet, og det ble redegjort for de rettslige rammene som følger av Grunnloven og EMK. Det ble ansett nødvendig å etablere tilstrekkelige sikkerhetsmekanismer for å ivareta de rettslige krav som følger av Grunnloven § 102 og EMK artikkel 8. I tillegg til å gi en klar hjemmel for behandlingen, måtte det etableres klare rammer for behandlingen slik at inngrepet overfor den enkelte ikke blir større enn nødvendig. Det måtte også etableres sikkerhetsmekanismer for å unngå misbruk, og det måtte sikres at EOS-utvalget kan føre tilstrekkelig kontroll med bruken. Omfanget av sikkerhetsmekanismer og kontroll måtte vurderes i lys av inngrepets alvor. Departementet anså det i den sammenheng sentralt at det er tale om offentlig tilgjengelig informasjon som ikke innhentes ved bruk av tvangsmidler eller ved skjult overvåking.

Det ble uttalt at det er en risiko for at tiltaket vil kunne ha en nedkjølende effekt på ytringsfriheten, ved at den enkelte vil kunne modifisere eller sensurere ytringene sine, eller helt unnlate å ytre seg på internett, på grunn av frykt for eller kunnskap om at ytringene vil kunne lagres hos PST. Etter departementets skjønn ville imidlertid tiltaket være en grunnleggende forutsetning for at PST skal kunne ivareta etterretningsoppdraget. Risikoen for en eventuell nedkjølende effekt kunne etter departementets syn ikke tillegges avgjørende vekt. På samme vis som inngrepet i retten til privatliv vil kunne anses rettferdiggjort etter EMK artikkel 8 nr. 2, la departementet til grunn at en eventuell dempende effekt på den frie meningsytringen i sin alminnelighet kan anses rettferdiggjort etter EMK artikkel 10 nr. 2 av hensyn til å bekjempe alvorlig kriminalitet og ivareta nasjonal sikkerhet. Hensynet til personvernet ble også ansett tilstrekkelig ivaretatt.

8.1.2 Høringsinstansenes syn

Forsvarsdepartementet, Politiets sikkerhetstjeneste (PST), Direktoratet for samfunnssikkerhet og bered-

skap (DSB), Det nasjonale statsadvokatembetet og *Finnmark politidistrikt* støtter forslaget.

Riksadvokaten viser til at forslaget reiser vanskelige spørsmål om avveining av ulike og til dels sterkt motstridende hensyn, men understreker betydningen av at PST gis rammebetingelser som gjør det mulig for tjenesten å utføre sitt samfunnsoppdrag på en fullgod måte. Tatt i betraktning dagens bruk av moderne informasjonsteknologi, sier det seg nærmest selv at PST som ledd i sin virksomhet i stor utstrekning må ha anledning til å gjøre bruk av informasjon som er åpent tilgjengelig på internett. I den grad PST ikke kan nyttiggjøre seg relevante opplysninger uten at også opplysninger uten betydning følger med, mener riksadvokaten at det i stor utstrekning må aksepteres at tjenesten behandler slik overskuddsinformasjon.

Utstrakt registrering av overskuddsinformasjon vil imidlertid kunne innebære inngrep i grunnleggende friheter og menneskerettigheter. Det er dermed av største betydning at slik behandling har grunnlag i klar lovhjemmel og skjer innenfor klare rettslige rammer, som ikke åpner for behandling utover det som er nødvendig og forholdsmessig, samt ivaretar behovet for kontroll mv.

PST støtter forslaget. Internett er en enorm kilde til informasjon om nesten alle former for aktivitet i samfunnet. Dette er informasjon en sikkerhets- og etterretningstjeneste forventes å nyttiggjøre seg. For å kunne forutse fremtidige endringer både i trusselbildet og på aktørsiden må PST være tilstede på denne arenaen. Det er ikke mulig å «følge med» ved å «se på» nettet i sanntid. På grunn av åpne kilders karakter må opplysningene som er relevante lagres og bearbeides over tid.

Innføring av regler som gir adgang til bruk av informasjon fra åpne kilder, må nedfelles i lov for ikke å komme i konflikt med enkeltpersoners grunnleggende rettigheter. Regelverket må finne sin balanse mellom hensynet til samfunnets behov for sikkerhet og enkeltindividers personvern, og det må inneholde rettssikkerhetsgarantier og kontrollmekanismer.

Politidirektoratet uttaler at lovforslaget fordrer en balansering av hensynet til personvern og ytringsfrihet på den ene siden og hensynet til sikkerhet på den andre siden, som med fordel kunne vært grundigere drøftet i høringsnotatet. Politidirektoratet etterlyser en nærmere vurdering av hvilken overføringsverdi dommene *Big Brother Watch og andre mot Storbritannia* og *Centrum för Rättvisa mot Sverige* har til departementets forslag.

Politidirektoratet og *Kripos* mener at Europarådskonvensjon nr. 108 om personvern med tilleggsprotokoller bør vurderes nærmere i det videre arbeidet.

Stortingets kontrollutvalg for etterretnings-, overvåkings- og sikkerhetstjeneste (EOS-utvalget) peker på at i *Big Brother Watch og andre mot Storbritannia* og *Centrum för Rättvisa mot Sverige* har EMD utviklet et sett med vurderingskriterier som er mer tilpasset innsamling av store datamengder (bulk) enn i tidligere rettspraksis. Særlig viktig er prinsippet om «end-to-end-safeguards». Selv om de to sakene gjaldt utenlandsetterretning (kommunikasjon ut og inn av landet), er mange av betraktningene like relevante for innenlandsetterretning, som tradisjonelt blir ansett som enda mer inngripende. Det er riktig nok en vesentlig forskjell mellom innsamling og lagring av hemmelig og åpent tilgjengelig informasjon. Utvalget mener likevel at forskjellen er mindre vesentlig enn høringsnotatet kan gi inntrykk av. Utvalget reiser spørsmål ved om inngrepet burde vært ledsaget av ytterligere vilkår for å ivareta borgernes personvern og rettsikkerhet – og i forlengelsen sikre mulighet for reell kontroll fra utvalget.

Datatilsynet viser til at forslaget berører sentrale spørsmål knyttet til personvern, ytringsfrihet og sikkerhet som krever en grundig utredning og avveining. Forslaget må sees i sammenheng med andre større overvåkingstiltak som politiet og etterretningstjenesten har fått hjemmel til, så som tilrettelagt innhenting i form av lagring av metadata om internettbruk, lagring av IP-adresser og overvåking av flypassasjerer. Samlet sett innebærer dette at myndighetenes mulighet til å overvåke borgerne har blitt betydelig utvidet de siste årene.

Datatilsynet ser at PST har et behov for å følge med og etterforske på internett. På grunn av det betydelige overvåkingspotensialet som digital overvåking med de muligheter kunstig intelligens og andre stordataverktøy åpner for, må imidlertid denne aktiviteten foregå under streng kontroll og rammer for den enkeltes rettsikkerhet. Forslaget utgjør et betydelig større inngrep i norske borgeres privatliv enn det departementet gir utrykk for, og skadepotensialet for vårt demokratiske samfunn er utvilsomt tilstede. Datatilsynet mener at konsekvensene av forslaget kan bli for store og at det derfor ikke bør innføres i sin nåværende form.

Tilsynet mener det er nødvendig å se på om *Big Brother Watch og andre mot Storbritannia* og *Centrum för Rättvisa mot Sverige* vil få anvendelse på innhenting fra åpne kilder, og at prinsippene fra disse dommene må legges til grunn. Etter Datatil-

synets syn er forslaget ikke i samsvar med praksis fra EMD og EU-domstolen om masseinnsamling av personopplysninger til bruk for etterretnings- og politiformål.

I høringsnotatet er det lagt vekt på at masseinnhenting fra åpne kilder i stor grad skiller seg fra hemmelig overvåking, uten at dette er nærmere grunngitt. Det kan synes som om det legges vekt på at bulkinnhenting av kommunikasjonsdata er mer å regne som «skjult» enn innhenting fra åpne kilder. Når det gjelder bulkinnhenting, er det allment kjent gjennom blant annet lov om etterretningstjenesten at den foregår og hva den på et generelt nivå samler inn. Det som er hemmelig er hvordan opplysningene behandles, hvilke søkekriterier som legges til grunn og hvem som er gjenstand for en nærmere undersøkelse. I tillegg er den enkeltes rettigheter, som underretning om registrering og rett til innsyn, begrenset. Dette vil i stor grad også gjelde for PSTs innhenting fra åpne kilder. Det kan derfor argumenteres for at prinsippene fra EMDs dommer får anvendelse.

Datatilsynet mener at en løsning hvor innhentingen er målrettet og underlagt en uavhengig forhåndskontroll også vil være mer i tråd med EU-retten, herunder avgjørelsen i *La Quadrature du Net and Others* (sak C-511/18).

Når det gjelder lovskravet, mener Datatilsynet at det er vanskelig å forstå begrepet åpent tilgjengelig og hvor omfattende innsamlingen skal være. På grunn av vag begrepsbruk i lovforslaget, samt uklarheter om hvem som omfattes, er det stor usikkerhet rundt hvem som faktisk rammes. Dette gjør at Datatilsynet mener at kravet til klarhet og forutberegnelighet neppe er oppfylt.

Datatilsynet mener at etterkontroll ved EOS-utvalget samlet sett ikke er et robust nok system for å verne mot misbruk, både fordi den er etterfølgende og fordi formålene er så vide at det er vanskelig å se hvilken del av PSTs kjernevirksomhet som ikke vil kunne benytte seg av opplysningene. Dette vanskeliggjør kontroll. Forslaget innebærer også unntak fra rettsikkerhetsgarantier som underretning og innsyn.

Datatilsynet vurderer at forslaget samlet sett ikke er i tråd med EMDs krav om ende-til-ende-kontroll, som blant annet innebærer uavhengig forhåndskontroll også av innhentingen og søkene som en sentral rettsikkerhetsmekanisme. Det mangler også en målrettethet og begrensning av innsamlingen.

Norges institusjon for menneskerettigheter (NIM) mener at flere sentrale problemstillinger og momenter ikke er tilstrekkelig berørt. Det savnes en bredere diskusjon om PSTs behov for å lagre så store mengder opplysninger, og avveiningen mot de sentrale menneskerettighetene dette berører. NIM mener forslaget er mer inngripende enn departementet legger til grunn. Masseinnsamling av data fra internett vil utfordre grunnleggende menneskerettigheter, som retten til privatliv, personvern og ytringsfriheten. Det bør derfor begrunnes mer inngående hvorvidt behandlingen er nødvendig i så stor utstrekning som foreslått. Etter NIMs oppfatning vil forslaget ikke være forholdsmessig slik det foreligger.

NIM mener at EMD-dommene *Big Brother Watch og andre mot Storbritannia* og *Center för Rättvisa mot Sverige* i noen grad gir veiledning om hvilke krav som stilles til den type innsamling og behandling som forslaget legger opp til. Det kan ikke utledes direkte av EMDs praksis at prinsippene for bulkovervåking ikke kommer til anvendelse for innhenting fra åpne kilder. Det forhold at forslaget gjelder åpne kilder kan også medføre at det stilles andre eller strengere krav.

I *Big Brother Watch og andre mot Storbritannia* stilles det opp åtte kriterier for bulkovervåkingssystemer. Videre legger dommen opp til en samlet vurdering. Etter NIMs syn har flere av prinsippene oppstilt i dommen overføringsverdi til dette tilfellet. Selv om selve innsamlingsmetoden er ulik og det er andre data som samles inn, vil forvaltning, sammenstilling, analyse, lagring samt senere bruk av dataene, i mindre grad skille seg fra problemstillingene i EMD-dommene, hvor poenget er å forhindre misbruksfaren som alltid foreligger ved slike personverninngrep.

Bruk av analyseverktøy kan frembringe nye mønstre og ny informasjon med utgangspunkt i de åpne kildene. Denne informasjonen kan være gjenstand for feilslutninger, og den kan ikke imøtegås. Problemstillingene som oppstår etter at opplysningene er samlet inn, skiller seg følgelig i liten grad fra problemstillingene i EMD-dommene.

NIM mener at høringsnotatet ikke i tilstrekkelig grad drøfter hvor tyngende inngrepet er, og hvilke rettssikkerhetsmekanismer som bør ledsage forslaget for at tiltaket skal kunne anses som forholdsmessig. Det er heller ikke drøftet om forskjellen mellom innsamling av informasjon om henholdsvis utenlandske aktører og egne borgere, påvirker inngrepsgraden. NIM mener at den vide innsamlingsadgangen, den lange lagringstiden, vide rammer for bruk, kombinert med bruken av automatiserte analyseverktøy, tilsier at forslaget må ledsages av strengere regler for lagring og andre rettssikkerhetsgarantier.

NIM legger til grunn at retten til et effektivt rettsmiddel på stadiet der innsamlingen eller behandlingen av opplysningene fortsatt er hemmelig, vil måtte ivaretas av EOS-utvalget. På bakgrunn av EOS-utvalgets høringsuttalelse ber NIM departementet vurdere hvorvidt utvalgets kontroll på dette punkt vil være tilstrekkelig som sikkerhetsmekanisme. NIM etterlyser en nærmere vurdering av hvordan retten til et effektivt rettsmiddel skal ivaretas, herunder hvordan ulik rettspraksis fra EMD har overføringsverdi til vår sak, og hvordan retten til et effektivt rettsmiddel skal sikres på de ulike stadiene av prosessen.

NIM etterlyser en grundigere vurdering av hvordan forslaget vil kunne virke nedkjølende på individers ønske om å ytre seg, særlig på nett, og hvilke samfunnsmessige konsekvenser dette kan få. NIM etterlyser også en grundigere redegjørelse for hvorvidt dette eventuelt vil påvirke samfunnet og demokratiet mer overordnet, og i hvilken grad dette avveies mot de formål forslaget søker å oppnå. NIM minner om at selv muligheten for en tendens i denne retning er ansett som et avgjørende argument i norsk rett.

Det er ikke utenkelig at masseinnsamling av informasjon på internett vil kunne utgjøre et inngrep i kildevernet og ha en nedkjølende effekt på fremtidige kilder ved at systemer for kunstig intelligens med stor informasjonstilgang har kapasitet til å identifisere og gjenkjenne hvem som er avsender av en skjult melding. NIM ber departementet vurdere og klargjøre at forslaget tar høyde for pressens kildevern i det videre arbeidet. Det bør videre foretas en drøftelse av kilders tillit til at de kan ha fortrolig kommunikasjon med journalister. Dette vil gjelde uavhengig av om forslaget direkte rammer kommunikasjon mellom kilder og journalister, ettersom eksistensen av stadig flere tiltak vil kunne etterlate et inntrykk av at slik kommunikasjon overvåkes av offentlige myndigheter. Denne ytterligere «nedkjølingseffekten» er noe som bør adresseres eksplisitt.

Medietilsynets vurdering er at de foreslåtte regelverksendringer medfører en betydelig inngripen i privatlivet og ytringsfriheten, noe som krever en langt mer omfattende begrunnelse enn høringsnotatet legger opp til. Medietilsynet mener at inngrepet i ytringsfriheten er større enn notatet tar høyde for, og at begrunnelsen for regelverksforslagene ikke står i forhold til inngrepet i ytringsfriheten og privatlivet. Medietilsynet kan derfor ikke støtte forslaget i sin nåværende form. Det er behov for å avklare hvordan kildevernet kan ivaretas, og hvordan risikoen for nedkjølingseffekter, særlig for redaktørstyrte medier, kan reduseres.

Advokatforeningen mener at flere sider av saken er utilstrekkelig utredet, herunder potensielle negativer konsekvenser for barn, nedkjølende effekter samt forholdsmessighetsvurderinger. Foreningen er bekymret for at en slik innsamling og lagring av informasjon for etterretningsformål vil ha en nedkjølende effekt på demokratiet og informasjonssamfunnet, for eksempel kritikk av myndighetene. Forslaget har både menneskerettslige og personvernmessige betenkeligheter. EMDs uttalelser i saker om bulkinnsamling om at inngrepet i individets rettigheter etter EMK artikkel 8 tiltar underveis i prosessen, er overførbare. Relevante likheter og forskjeller er ikke beskrevet og analysert nærmere. Innsamlingen og potensiell bruk av opplysningene vil åpenbart medføre at inngrepet i individets rettigheter tiltar etter hvert som det gjøres søk i opplysningene og disse benyttes for formålene.

UTSYN mener det burde vært grundigere vurdert hvordan lovforslaget kan virke nedkjølende på samfunnsdebatten og deltakernes vilje til å ytre seg. Et lovforslag som griper direkte inn i forholdet mellom stat og borger og som sterkt berører ytringsfriheten, må være grundig utredet. Også *Tekna* og *NITO* er bekymret for den nedkjølende effekten av forslaget. NITO mener at det er hensiktsmessig å avvente ytringsfrihetskommisjonens vurdering av overvåkingens konsekvens for ytringsfriheten.

IKT-Norge er spesielt opptatt av nødvendigheten av kritiske vurderinger og gode begrunnelser på grunn av faren for redusert tillit og nedkjølingseffekt som overvåking kan ha på bruken av digitale tjenester. Etter deres syn er vurderingen av nedkjølingseffekten for overfladisk. Betydningen forslaget har for tilliten til digitaliserte tjenester, samt betydningen av at frimodige ytringer kan bli sensurert, er ikke drøftet. Faren for nedkjølingseffekt er reell, og slik effekt vil kunne være skadelig for både norsk offentlig debatt og norsk næringsliv.

Elektronisk Forpost Norge mener at forslaget legger opp til svært omfattende overvåking av, i praksis, alle landets borgere.

8.1.3 Departementets vurderinger

Departementet har merket seg at en rekke høringsinstanser har forståelse for behovet for forslagene, selv om de ikke nødvendigvis støtter den innretningen som er foreslått. Departementet fastholder at det er behov for at PST kan lagre, analy-

sere og systematisere åpent tilgjengelig informasjon for å utarbeide analyser og etterretningsvurderinger om forhold i Norge som kan true nasjonale sikkerhetsinteresser. Dagens teknologiske virkelighet gjør at stadig mer informasjon nå kun finnes på nett, og at trusselaktørene i økende grad flytter sin aktivitet fra det fysiske til det digitale rom. Lagring, analyse og sammenstilling av åpent tilgjengelig informasjon er derfor etter departementets syn et sentralt verktøy for at PST skal kunne ivareta oppgaven med å utarbeide analyser og etterretningsvurderinger, slik denne oppgaven er beskrevet i punkt 7 i denne proposisjonen. Ved å endre formuleringen av oppgaven som innenlands etterretningstjeneste, blir det etter departementets syn også klarere hva hjemmelen for behandling av åpent tilgjengelig informasjon er ment brukt til.

Flere høringsinstanser er uenige i departementets vurdering av at dommene fra EMD i *Big Brother Watch og andre mot Storbritannia* og *Center för Rättvisa mot Sverige* har begrenset overføringsverdi til forslaget, og de etterlyser en grundigere vurdering av disse dommene. Informasjonen som kan behandles etter forslaget her skiller seg fra informasjonen det er snakk om i EMD-dommene, ved at forslaget her er begrenset til åpent tilgjengelig informasjon. Informasjon som ligger i åpne kilder er åpent tilgjengelig for alle, og det eksisterer etter departementets syn ikke en berettiget forventning om samme vern for slik informasjon som for opplysninger som ikke er åpent tilgjengelige. Departementet opprettholder derfor vurderingen av at dommene ikke har direkte overføringsverdi. Med de justeringene som foreslås i punktene nedenfor, blir også parallellen til bulkinnsamling av grensekryssende informasjon (tilrettelagt innhenting) mindre treffende enn det høringsinstansene synes å legge til grunn. I den grad det kan trekkes en parallell til E-tjenestens virkemidler, mener departementet at det er mer nærliggende å sammenligne forslaget med E-tjenestens muligheter til å innhente rådata i bulk i form av åpent tilgjengelig informasjon, jf. etterretningstjenesteloven §§ 5-3 og 6-2. Slik innhenting kan også berøre norske borgere, jf. § 4-4 som åpner for innhenting fra åpne kilder selv om informasjonen er publisert av eller på annen måte berører personer i Norge.

Etter forslaget her vil innhentingen rammes inn ved at behandlingen må antas å være nødvendig for utarbeidelse av analyser og etterretningsvurderinger, jf. omtalen i punkt 8.3.3. Dette vurderes som sammenlignbart med kravene i etterretningstjenesteloven § 5-3 om at innhenting kan skje for å få tilgang til et «relevant og tilstrekkelig informasjonsgrunnlag». Behandlingen vil med andre ord være mer målrettet enn tilrettelagt innhenting. For innhenting av rådata i bulk er det ikke etablert et regime med uavhengig forhåndskontroll, og det er heller ikke etablert særlige beføyelser for EOS-utvalget. Departementet vil likevel kommentere kravene som er oppstilt i *Big Brother Watch og andre mot Storbritannia* og *Center för Rättvisa mot Sverige* i de senere punktene i denne proposisjonen der disse er relevante.

Innrammingen vil også bidra til å ivareta Ytringsfrihetskommisjonens vurderinger i NOU 2022: 9 En åpen og opplyst offentlig samtale – Ytringsfrihetskommisjonens utredning. Kommisjonen advarer i punkt 7.9.8 side 128 mot bruk av generelle og vidtrekkende lovbestemmelser på områder som kan påvirke ytringsfriheten. Etter kommisjonens syn var forslaget som ble sendt på høring for generelt utformet. Forslaget som fremmes i denne proposisjonen er innrettet på en mer målrettet måte enn høringsforslaget.

Flere høringsinstanser har etterlyst en grundigere vurdering av den nedkjølende effekten av forslaget og inngrepet i ytringsfriheten, herunder ivaretakelse av pressens kildevern. Departementet ser at forslaget vil kunne ha en nedkjølende effekt ved at personer vil kunne unnlate å ytre seg av frykt for at opplysningene blir lagret hos PST. Selv om forslaget ikke legger begrensninger på retten til å ytre seg, kan det derfor like fullt gripe inn i ytringsfriheten. Inngrep kan være tillatt dersom det har hjemmel i lov, ivaretar et legitimt formål og er nødvendig i et demokratisk samfunn. Departementet mener at kravene som kan utledes av EMK artikkel 10 og Grunnloven § 100 er ivaretatt i forslaget her, og at tiltaket er nødvendig og forholdsmessig, særlig i lys av de endringene som nå er foreslått og rettssikkerhetsmekanismene det legges opp til i kombinasjon med allerede gjeldende regelverk.

PST og det øvrige politiet har også i dag mulighet til å følge med på ytringer på internett, og dersom politiregisterlovens regler er oppfylt, registrere disse. Det må derfor antas at de som vil unnlate å ytre seg som følge av forslagene her, til en viss grad lar være allerede i dag. En stor del av PSTs arbeid er knyttet til å verifisere informasjon og å ta ned bekymringer om personer som man tror kan utgjøre en trussel. Således kan det være i personens egen interesse at PST har et tilstrekkelig informasjonsgrunnlag til å kunne konkludere med at vedkommende ikke utgjør en trussel eller bør registreres. Dette kan være vel så viktig for å

sikre at PST evner å gi riktig beslutningstøtte om omfang og utvikling av trusler.

Enkelte høringsinstanser har etterlyst en vurdering av om forslaget ivaretar kildevernet. Kildevernet omfatter journalistisk materiale som direkte eller indirekte kan avsløre identiteten til en kilde som journalisten har benyttet. Vernet omfatter opplysninger som kan identifisere kilden ved navn, bilde eller annen personidentifikasjon, samt uredigert og upublisert materiale såfremt informasjonen kan avsløre journalistens kilder. Forslaget i denne lovproposisjonen er begrenset til åpent tilgjengelig informasjon. Informasjon er ikke åpent tilgjengelig dersom den er beskyttet av passord eller andre sikkerhetsmekanismer, og informasjonen er heller ikke åpent tilgjengelig dersom tilgang krever aktivt fordekt opptreden. Opplysningene som kan behandles etter forslaget er med andre ord opplysninger som hvem som helst kan få tilgang til, og som dermed ikke kan forventes å holdes fortrolig. Det er etter departementets syn tvilsomt om opplysninger som er åpent tilgjengelig i det hele tatt vil være av en slik art at de er omfattet av kildevernet. I den grad korrespondanse mellom pressen og en kilde vil behandles etter den nye bestemmelsen, må denne korrespondansen ha foregått på en plattform som er allment tilgjengelig for offentligheten. Det har etter departementets syn formodningen mot seg at fortrolig kommunikasjon med kilder foregår på offentlig tilgjengelige plattformer i særlig omfang. Spørsmålet om vern om fortrolige kilder kommer derfor neppe på spissen.

Høringsinstansene som uttrykker bekymring for pressens kildevern, viser særlig til at automatiserte analyser og bruk av kunstig intelligens kan avsløre hvem som snakker med hvem. Etter forslaget kan automatiserte analyseverktøy bare benyttes ved utarbeidelse av analyser og etterretningsvurderinger om forhold i Norge som kan true nasjonale sikkerhetsinteresser. I disse tilfellene er bruken av analyseverktøyene ikke rettet mot enkeltpersoner eller kartlegging av deres aktivitet, jf. omtalen i punkt 8.9.3 nedenfor. Også av denne grunn mener departementet at forslaget ikke vil gripe inn i kildevernet.

Etter departementets syn er kravet til effektive rettsmidler ivaretatt med det alminnelige systemet med EOS-utvalgets kontroll og mulighetene for å reise sak for domstolene. EOS-utvalget skal sikre at PSTs virksomhet holdes innenfor rammen av tjenestens fastlagte oppgaver og føre kontroll med tjenestens behandling av forebyggende saker og etterforskningssaker, dens bruk av skjulte tvangsmidler og andre skjulte metoder for informasjonsinnhenting. Dette vil også omfatte kontroll med PSTs bruk av den nye bestemmelsen. Departementet forutsetter at PST legger særskilt til rette for utvalgets kontroll av behandlingen som forslaget her åpner for.

Som omtalt i punkt 5.3 ovenfor åpner Europarådskonvensjon nr. 108 om personvern i forbindelse med elektronisk databehandling av personopplysninger med senere tilleggsprotokoller for en rekke unntak når behandlingen skjer av hensyn til nasjonal sikkerhet eller kriminalitetsbekjempelse, dersom det følger av lov og er et nødvendig tiltak i et demokratisk samfunn. Forslaget i denne proposisjonen er innenfor unntaksmulighetene som konvensjonen åpner for, og er dermed etter departementets vurdering i tråd med konvensjonens krav.

Samlet sett mener departementet at forslaget er i tråd med de krav som kan utledes av Grunnloven, EMK og EMDs praksis. Forslaget ivaretar et legitimt formål og går etter departementets syn ikke lenger enn nødvendig. De sikkerhetsmekanismer som foreslår i proposisjonen her, kombinert med de mekanismer som allerede finnes i regelverket og EOS-utvalgets kontroll med tjenesten, ivaretar også kravene til nødvendige sikkerhetsmekanismer.

8.2 Hva menes med åpent tilgjengelig informasjon?

8.2.1 Forslaget i høringsnotatet

Forslaget i høringsnotatet var begrenset til behandling av åpent tilgjengelig informasjon. Med åpent tilgjengelig informasjon menes informasjon som er allment tilgjengelig for offentligheten, i hovedsak informasjon i det digitale rom. Det er ikke avgjørende hvor eller på hvilken måte informasjonen er gjort åpent tilgjengelig. Åpent tilgjengelig informasjon omfatter for eksempel nettavisartikler, åpne offentlige registre, åpne diskusjoner i sosiale medier, kommentarfelt, blogger mv. Hvorvidt et nettsted kan anses som offentlig tilgjengelig, vil bero på om og i hvilken grad det utøves en reell kontroll med tilgangen til nettstedet. Informasjon regnes derfor som åpen selv om det kreves et abonnement eller registrering for å få tilgang, for eksempel et abonnement på en nettavis eller at det må opprettes en bruker på sosiale medier.

Informasjon regnes som åpent tilgjengelig selv om den er publisert på «det mørke nettet» og ikke er tilgjengelig gjennom vanlige søkemotorer, med mindre det er etablert spesielle mekanismer for å

beskytte innholdet. Kryptert informasjon kan være åpent tilgjengelig hvis enhver kan laste den ned, for eksempel hvis en bruker på et åpent forum laster opp en kryptert fil som andre brukere fritt kan laste ned.

Avgrensningen til åpent tilgjengelig informasjon innebærer at for eksempel informasjon publisert på lukkede nettsteder eller private samtaler på chattetjenester, e-poster eller annen kryptert eller privat kommunikasjon, ikke omfattes.

I høringsnotatet ble det vist til at det er vanskelig å angi uttømmende hva som kan anses som åpent tilgjengelig informasjon. Det ble derfor foreslått en negativ avgrensning etter mal av etterretningstjenesteloven § 6-2, som fastsetter at informasjon ikke er åpent tilgjengelig dersom tilgang til informasjonen krever forsering av passord eller andre lignende beskyttelsesmekanismer.

8.2.2 Høringsinstansenes syn

Datatilsynet, Norges institusjon for menneskerettigheter (NIM), Advokatforeningen, Den Norske Dataforening og *Tekna* etterlyser en tilsvarende avgrensning som i etterretningstjenesteloven § 6-2 om at informasjon ikke er åpent tilgjengelig dersom tilgang krever «aktivt fordekt opptreden». Det stilles spørsmål ved hvorfor ikke denne begrensningen er med, og det er dermed uklart om PST vil kunne benytte seg av falske identiteter eller brukere på nett for å få tilgang til informasjon som en bruker av sosiale medier kun deler med venner, følgere eller en liknende avgrenset krets. Avgrensning mot bruk av aktivt fordekt opptreden bør omtales og reguleres tydelig.

Politidirektoratet og *Kripos* støtter at begrepet «åpent tilgjengelig informasjon» defineres i lovforslaget. De mener at det bør inntas en definisjon av begrepet «åpent tilgjengelig informasjon» i politiregisterloven § 2 om definisjoner.

Datatilsynet mener det fremstår som om forslaget hviler på en antakelse om at informasjon som finnes på internett ofte eller i hovedsak er selvpublisert. Internett fungerer ikke alltid på denne måten. Falske kontoer kan opprettes. Beskyldninger og karakteristikker av andre brukere hagler i kommentarfeltet. Intim og personlig informasjon kan bli ulovlig tilgjengeliggjort, og brukere kan bli «doxxet» mot sin vilje – det vil si at personopplysninger blir samlet inn og publisert for å ramme enkeltpersoner.

Tilsynet viser til at selv om deler av «det mørke nettet» er kryptert og krever ulike typer autorisasjon for å få tilgang til informasjon og nettsteder, brukes det også til fritt å utveksle opplysninger til bruk for eksempelvis hackere, publisering etter løsepengeangrep hvor løsepenger ikke ble betalt og til å publisere materiale, herunder taushetsbelagt informasjon, etter datainnbrudd. Ved større og flere lekkasjer, med tilsvarende lang lagringstid, kan det i realiteten bli langt mer informasjon om enkeltpersoner enn hva som postes online og er søkbart gjennom tradisjonelle søkemotorer. Også *Medietilsynet* og *Tekna* peker på disse forholdene.

Datatilsynet savner en prinsipiell vurdering av hva som er å anse som åpent tilgjengelig. Vurderingen bør ta utgangspunkt i behovet for vern av ytringsfrihet og privatliv, veid opp mot myndighetenes behov for overvåking av elementer som kan anses som en trussel mot samfunnet. I stedet for en tilnærming hvor alt anses åpent tilgjengelig dersom ikke brukerne selv aktivt har tatt grep for å beskytte opplysningene, kan definisjonen ta utgangspunkt i en generell vurdering av hva som er ytret i det offentlige rom. Som eksempel nevnes straffeloven § 10, som definerer offentlig sted og offentlig handling i straffelovens forstand.

Borgernes forventning om å kunne ytre seg fritt utenfor myndighetenes kontroll, vil trolig være større i mindre fora enn i grupper eller steder som når ut til en større krets. Datatilsynet vil påpeke at uavhengig av definisjonen vil en omfattende registrering av ytringer fremsatt i det offentlige rom kunne ha negative konsekvenser.

Et perspektiv som ikke i tilstrekkelig grad er drøftet er hvordan en automatisert innsamling og analyse av ytringer og handlinger som for eksempel å være medlem av en gruppe vil kunne gi opplysninger som den enkelte ikke ønsker å dele med offentligheten.

Det må også fremgå klart at informasjon som ikke er lagt ut på nettet i tråd med personvernforordningen eller som er taushetsbelagt ikke kan anses som «åpent tilgjengelig informasjon». I så fall vil personer som mot sin vilje har fått lagt ut informasjon på nettet og i strid med taushetsplikt ha et dårligere vern mot inngrep i privatlivet fra PST enn andre.

NIM viser til at begrepet «åpent tilgjengelig informasjon» ikke er nærmere definert eller avgrenset utover at det ikke skal kreve «forsering av passord eller lignende beskyttelsesmekanismer». Forslaget åpner for innsamling av personopplysninger og annen informasjon om enhver, uten at de noen gang har vært eller vil være i politiets søkelys. Dette kan inkludere sensitive personopplysninger. Videre vil det kunne inkludere offentlig tilgjengelige opplysninger som kan være feilaktige eller misvisende, opplysninger som er

tilveiebrakt eller publisert ulovlig og opplysninger publisert om enkeltpersoner uten deres kjennskap eller samtykke. Dette er opplysninger som det vil kunne være vanskelig for den det gjelder å ha kjennskap til, eksempelvis der opplysningene er publisert på sider som ikke er indeksert via søkemotorer, eller på det mørke nettet. Forutsetningen om at noe er publisert åpent, og at det dermed implisitt er gitt samtykke til at andre kan få kjennskap til opplysningene, slår ikke til for denne typen opplysninger.

NIM anser at innsamling og lagring av informasjon og aktivitet i sosiale medier reiser særlige spørsmål. Selv om informasjon publisert i sosiale medier etter lovforslaget vil kunne kategoriseres som «åpent tilgjengelig», er det grunn til å anta at befolkningen kan oppfatte denne typen informasjon som mer privat enn informasjon som fremgår av andre åpne kilder. Hva som deles offentlig i sosiale medier kan dessuten avhenge av hvilke brukerinnstillinger hver enkelt har valgt og endringer i plattformens brukervilkår. Dette gjør at den enkelte kan ha varierende innsikt i hva som deles med offentligheten.

Medietilsynet mener at definisjonen av «åpent tilgjengelig informasjon» fremstår som upresis, og at det er vanskelig å forstå rekkevidden av endringene og omfanget av datainnsamlingen. Definisjonen må i større grad presiseres og avgrenses. Informasjon på det mørke nettet oppfattes ikke som allment tilgjengelig, noe som illustrerer at departementets forståelse av «åpent tilgjengelig» trolig er avvikende fra befolkningens.

Advokatforeningen oppfatter at begrepet «åpent tilgjengelig informasjon» skal forstås svært vidt og antar at PST i praksis kan samle inn og lagre alt som er observerbart. Advokatforeningen er bekymret for at en slik innsamling og lagring av informasjon for etterretningsformål vil ha en nedkjølende effekt på demokratiet og informasjonssamfunnet, for eksempel kritikk av myndighetene. Resultatet kan være at vi reduserer eller fjerner offentlige debatter som vi ønsker å ha i det åpne rom, selv om det kan være ubehagelige ytringer.

Også Advokatforeningen påpeker at forslagets definisjon av åpent tilgjengelig informasjon ikke nødvendigvis gjenspeiler befolkningens oppfatning av hvilken informasjon som er offentlig og åpen. Det er glidende overganger fra informasjon som er fremsatt i private nettfora til generell informasjon fremsatt på en offentlig arena rettet mot et bredt publikum. Det er etter Advokatforeningens syn svært viktig at departementet klargjør hvilke grenser som gjelder for PSTs informasjonsinnhenting. En negativ avgrensing er lite egnet til dette. Videre mener foreningen at begrepet «lignende beskyttelsesmekanismer» er uklart og vanskelig å forstå. Legalitetsprinsippet tilsier at PSTs adgang til å gripe inn i den private sfæren må være klart angitt.

Advokatforeningen fremhever at en slik hjemmel for PST kan føre til at kriminaliteten går over i lukkede fora hvor dialogen er beskyttet av passord eller andre beskyttelsesmekanismer. Dette synes i begrenset grad å være utredet av departementet. Også *IKT-Norge* og *NITO* peker på disse forholdene.

Rettspolitisk forening mener definisjonen er vid, og lett kan ramme informasjon som avsenderen har ment å holde privat, for eksempel i små grupper på sosiale medier som ikke er lagt bak en teknisk beskyttelsesmekanisme. Den enkeltes forventning om privatliv er et vesentlig element i vurderingen av hvor inngripende et tiltak er. Den vide definisjonen av «åpent tilgjengelig informasjon» må antas å i seg selv ha en nedkjølende effekt på den enkeltes meningsytringer. Avgrensningen av hva som skal regnes som offentlig og privat bør både innstrammes og presiseres.

Tekna viser til at forslaget vil omfatte informasjon fra systemer som er hacket og delt på det mørke nettet, selv om dette er informasjon som aldri var ment å være offentlig tilgjengelig. Det oppstår da spørsmål om hvordan man har man tenkt å skille mellom informasjon som er lovlig og lovstridig lagt ut. Videre vil åpen informasjon ikke bare være informasjon man har lagt ut selv, men også informasjon andre har lagt ut uten at man selv har godkjent dette. Med lang lagringstid kan man også oppleve at informasjon som ikke er tilgjengelig for en selv eller andre fortsatt vil være tilgjengelig for etterretningen.

8.2.3 Departementets vurderinger

Angivelsen av hva som regnes som åpent tilgjengelig informasjon er ment å forstås på samme måte som etter etterretningstjenesteloven § 6-2. I høringsnotatet ble det vist til at det ikke er mulig å gi en uttømmende definisjon av begrepet. Høringsinnspillene har understreket dette.

Departementet er klar over at mye informasjon som er åpent tilgjengelig kan være publisert uten at personen det gjelder er kjent med det, eller at informasjonen er publisert urettmessig. Dersom man først åpner for at PST kan innhente åpent tilgjengelig informasjon uten en vurdering av om den enkelte opplysning i seg selv er nødvendig, kan det heller ikke avgrenses mot infor-

masjon som omhandler mindreårige, er lovstridig lagt ut, underlagt taushetsplikt eller lignende. Slike begrensninger gjør seg heller ikke gjeldende i andre sammenhenger der PST og politiet for øvrig behandler åpent tilgjengelig informasjon, så fremt politiregisterlovens regler ellers er oppfylt.

Det sentrale må derfor være at opplysningene rent faktisk er åpent tilgjengelig, det vil si at informasjonen er allment tilgjengelig for offentligheten. Hvordan eller hvorfor opplysningene er publisert er dermed uten betydning. Avgrensning av hvilke opplysninger som kan innhentes omtales i punkt 8.3.3 nedenfor.

Når det gjelder avgrensning mot behandling av informasjon der tilgang krever «aktivt fordekt opptreden», har det ikke vært hensikten med forslaget å åpne for at PST kan behandle opplysninger innhentet ved slik opptreden etter den nye bestemmelsen. Forslaget åpner dermed ikke for at en tjenesteperson eksempelvis utgir seg for å være en annen, ikke-fiktiv person og gjennom samhandling med mennesker oppnår tilgang til for eksempel et forum på Internett, Det åpnes heller ikke for at PST gjennom en fiktiv bruker kan opptre manipulerende for å få eller opprettholde tilgang til et lukket forum eller gruppe på et nettsamfunn. I lys av høringsinnspillene ser departementet at avgrensningen mot «aktivt fordekt opptreden» bør inntas i bestemmelsen, for å unngå tvil om hva som er ment med åpent tilgjengelig informasjon.

Advokatforeningen mener at begrepet «lignende beskyttelsesmekanismer» er uklart. Departementet viser til at begrepet benyttes i etterretningstjenesteloven § 6-2 og skal forstås på samme måte i denne bestemmelsen. Lignende beskyttelsesmekanismer omfatter andre beskyttelsestiltak enn passordbeskyttelse som gjør at informasjonen ikke er åpent tilgjengelig for allmennheten. Det kan eksempelvis være biometrisk autentisering, at informasjonen kun kan nås fra spesifikke fysiske enheter eller at den på andre måter er utilgjengelig for uvedkommende.

Departementet opprettholder etter dette en negativ avgrensning av hva som regnes som åpent tilgjengelig, på samme måte som etter etterretningstjenesteloven § 6-2. Det anses ikke hensiktsmessig med en definisjon av begrepet i politiregisterloven § 2. Begrepet benyttes kun i de reglene som gjelder PST, og forslaget er ikke en generell regulering av bruk av åpent tilgjengelig informasjon. Bestemmelsen får dermed ikke betydning for PSTs muligheter til å bruke åpent tilgjengelig informasjon i andre sammenhenger, eller for det øvrige politiets adgang til å benytte åpent tilgjengelig informasjon.

Risikoen for at personer som ønsker å skjule sin kommunikasjon kan flytte seg til plattformer som ikke er offentlig tilgjengelige er ikke ny med dette forslaget. Det er grunn til å tro at mange av disse allerede velger å benytte plattformer som ikke er åpent tilgjengelige. Dette er derfor etter departementets syn ikke et argument mot at PST skal få den muligheten som forslaget her legger opp til. Ved å kunne analysere, sammenstille og vurdere åpent tilgjengelig informasjon over tid vil PST like fullt kunne utarbeide gode analyser og etterretningsvurderinger, selv om enkelte personer vil avstå fra å ytre seg på åpne plattformer og deres ytringer derfor ikke vil finnes i informasjonsgrunnlaget.

8.3 Særskilt hjemmel for å behandle åpent tilgjengelig informasjon til etterretningsformål

8.3.1 Forslaget i høringsnotatet

I høringsnotatet ble det vist til at det er en forventning om at PST skal kunne «følge med» på internett for å avdekke ukjente trusselaktører, kartlegge utviklingen i trusselbildet og oppdage nye fenomener som kan medføre nye trusler. I dagens informasjonssamfunn kan denne forventningen vanskelig etterkommes uten at tjenesten gis anledning til å lagre, systematisere og analysere store mengder åpent tilgjengelig informasjon over tid. Det er ikke mulig å avdekke sammenhenger, se det store bildet eller «følge med» på en tilstrekkelig effektiv måte for å ivareta etterretningsoppdraget bare ved å være til stede på internett og med bruk av manuelle søk i sanntid.

Departementet mente derfor at det var behov for å åpne for at PST kan lagre, systematisere og analysere åpent tilgjengelig informasjon som ledd i tjenestens etterretningsvirksomhet. Dette ville gjøre at PST i større grad kan kartlegge utvikling, avdekke nye trender i trusselbildet og forutse fremtidige trusler i Norge. Det ville også bidra til å gi rettidig og relevant beslutningsstøtte slik at myndighetene kan vurdere trussel- og sårbarhetsreduserende tiltak der behovet gjør seg gjeldende. For tjenestens egen del vil åpent tilgjengelig informasjon være et viktig bidrag i vurderingen av hvilke trusler og trusselaktører det bør settes inn tiltak mot, og hvilke tiltak som vil være egnet.

Behandling av store mengder åpent tilgjengelig informasjon for etterretningsformål er ikke mulig innenfor de tradisjonelle behandlingsre-

glene i politiregisterloven fordi det meste av opplysningene som vil måtte behandles, vil være unødvendige, ikke-relevante opplysninger for tjenesten. Det var etter departementets syn behov for å etablere en egen hjemmel for denne typen behandling, og det ble foreslått en ny bestemmelse som regulerer alle sider ved behandlingen, inkludert en forskriftshjemmel som oppstiller et krav til nærmere regulering i forskrift.

I høringsnotatet ble det uttalt at departementet hadde vurdert om adgangen til å behandle offentlig tilgjengelig informasjon burde begrenses, for eksempel basert på konkrete informasjonsbehov eller lignende. Departementet mente imidlertid at en slik avgrensning ville være vanskelig å gjennomføre i praksis, og at det ikke ville være mulig å etablere egnede og tilstrekkelig presise avgrensingskriterier i regelverket for hvilke opplysninger som kan lastes ned. Det ble derfor ikke foreslått noen begrensninger i regelverket i hva som kan hentes inn, så lenge det er snakk om åpent tilgjengelig informasjon.

I høringsnotatet ble det vist til at det forekommer at åpen informasjon må lastes ned og lagres lokalt før det er mulig å foreta søk i innholdet. Slike datasett har blitt en viktig kilde til informasjon for akademia, journalister, kommersielle aktører, aktivister og organisasjoner i sivilsamfunnet. Etter departementets syn burde slik bruk av åpne kilder også være mulig for PST.

8.3.2 Høringsinstansenes syn

Forsvarsdepartementet støtter forslaget. Åpne kilder er i dagens informasjonssamfunn en relevant metode for å samle inn informasjon om flere av forholdene som PST skal forebygge og etterforske. Metoden vil mest sannsynlig komplementere andre metoder som PST kan benytte. Sett i sammenheng med tvangsmidlene som PST har tilgjengelig for å forebygge og etterforske saker, er metoden i seg selv ikke særlig inngripende. Ettersom innhentingen ikke skjer etter samtykke, og fordi summen av informasjonen over tid kan bli omfattende, kan innhentingen likevel bli inngripende i et personvernperspektiv selv om informasjonen er tilgjengeliggjort av personen selv. Forsvarsdepartementet støtter derfor forslaget om at metoden lovreguleres. Det bør også vurderes om politiets behandling av informasjon fra åpne kilder generelt bør reguleres.

Politiets sikkerhetstjeneste (PST) støtter forslaget. Det er ikke mulig å «følge med» ved å «se på» nettet i sanntid. På grunn av åpne kilders karakter må opplysningene som er relevante lagres og bearbeides over tid.

Riksadvokaten mener at tatt i betraktning dagens bruk av moderne informasjonsteknologi, sier det seg nærmest selv at PST som ledd i sin virksomhet i stor utstrekning må ha anledning til å gjøre bruk av informasjon som er åpent tilgjengelig på internett. I den grad relevante opplysninger ikke kan nyttiggjøres uten at også opplysninger uten betydning følger med, mener Riksadvokaten at det i stor utstrekning må aksepteres at tjenesten behandler slik overskuddsinformasjon.

Stortingets kontrollutvalg for etterretnings-, overvåkings- og sikkerhetstjeneste (EOS-utvalget) savner en vurdering av behovet for å lovfeste innhenting av åpent tilgjengelig informasjon som en metode for PST. Utvalget reiser spørsmål ved om inngrepet burde vært ledsaget av ytterligere vilkår for å ivareta borgernes personvern og rettsikkerhet – og i forlengelsen sikre mulighet for reell kontroll fra utvalget.

Datatilsynet ser at PST har et behov for å følge med og etterforske på internett, men på grunn av det betydelige overvåkingspotensialet som digital overvåking med de muligheter kunstig intelligens og andre stordataverktøy åpner for, må denne aktiviteten foregå under streng kontroll og rammer for den enkeltes rettsikkerhet. En løsning hvor innhentingen er målrettet og underlagt en uavhengig forhåndskontroll vil være mer i tråd med praksis fra EMD og EU-domstolen, der målretting står sentralt.

Tilsynet mener at innhentingsmetode burde vært drøftet. Det er ikke beskrevet hvordan PST skal innhente informasjon fra nettet, om dette skal gjøres manuelt og målrettet, gjennom verktøy utviklet av PST eller av underleverandører som tilbyr «skraping» av nettet. Det er heller ikke drøftet om det vil være tillatt å bruke såkalte «data brokers» som selger opplysninger fra apper eller nettet.

Norges institusjon for menneskerettigheter (NIM) mener at omfanget av den foreslåtte innsamlingen er iøynefallende. Etter NIMs oppfatning bør det vurderes om adgangen til innsamling av opplysninger bør presiseres og konkretiseres nærmere.

Bruk til etterretningsvirksomhet er et vidt virkeområde, og er ikke en entydig rettslig størrelse. Hvem eller hvordan det skal avgjøres om bruken kan rubriseres som «etterretningsvirksomhet», er ikke angitt. NIM forstår departementet dithen at «etterretning» blant annet skal omfatte innhenting, analyse og vurdering av informasjon, eksempelvis med formål å forebygge straffbare forhold, men også forut for det som tradisjonelt omfattes

av begrepet forebygging. Det er vanskelig for befolkningen å skulle overskue konsekvensene av dette, all den tid det er vanskelig å avgjøre hva som omfattes. Forslaget inneholder ikke noen begrensninger på hvordan søk skal foregå eller gjennomføres. Høringsnotatet burde inneholdt avgrensninger av hvilke søkekriterier som kan benyttes, og mekanismer for å sikre at disse står i saklig sammenheng med formålet opplysningene skal uthentes for. Hvilke søkebegrep som brukes kan være avgjørende for om en konkret bruk av informasjonen er forholdsmessig eller ikke.

Rettssikkerhetsmekanismene må fungere i praksis, herunder må garantiene mot misbruk bygges inn i systemet, og det må foreligge reelle avgrensninger av hvilke søkekriterier som kan benyttes. Slik forslaget er lagt opp, mener NIM at det gir PST en ubestemt skjønnsmyndighet uten kriterier for overprøving. Dette gjør også den foreslåtte kontrollen av søk lite effektiv som kontrollmekanisme, ettersom skillet mellom lovlig og ikke lovlige søk ikke er tydelig.

På bakgrunn av den vide innsamlingsadgangen og den lange lagringstiden anbefaler NIM at departementet legger til rette for forhåndskontroll når det foretas søk i det innsamlede materialet. Dette kan eventuelt gjøres ved at det innføres en godkjenningsordning for hvilke opplysninger, søkeord eller andre parametere som kan ligge til grunn for søk i materialet.

Medietilsynet savner en vurdering av om det identifiserte formålet kan oppnås på en mindre inngripende måte. Forslaget fremstår mer inngripende for privatlivet og ytringsfriheten enn hva som er tilfellet i de fleste land i Norden, uten en forklaring på om trusselbildet i Norge er vesensforskjellig fra våre naboland.

Også *Advokatforeningen* påpeker at det ikke er tilstrekkelig klargjort om forslaget om bulkinnsamling av åpen tilgjengelig informasjon samsvarer med eller går lengre enn lovhjemlene til etterretningstjenestene i land som Norge har tradisjon for å sammenligne seg med. Både fra et menneskerettighetsperspektiv og fra et personvernståsted ser Advokatforeningen betydelige betenkeligheter ved forslaget. Slik hjemmelen er utformet, vil det være opp til PST å avgjøre hvorvidt innsamlingen skjer i tråd med etterretningsformålet. En så vid formålsbeskrivelse innebærer i praksis ingen begrensning.

Advokatforeningen mener det burde vært utredet nærmere om adgangen til å behandle offentlig tilgjengelig informasjon bør begrenses. For eksempel kan det være aktuelt å begrense PSTs adgang til å samle inn og lagre åpent tilgjengelig informasjon om barn, som nyter en særskilt beskyttelse etter personvernregelverket.

Det rettslige kravet om at en behandling av personopplysninger skal være nødvendig betyr i utgangspunktet at terskelen er høy. Advokatforeningen har problemer med å se at det er mulig å ivareta kravet til nødvendighet samtidig som PST gis hjemler som foreslått.

Tekna anerkjenner PST sitt behov for å få nye verktøy for å møte digitale utfordringer og løse samfunnsoppdraget. De savner imidlertid en grundigere redegjørelse for hvilke verktøy og metoder som skal benyttes ved innhenting. Det er uklart om dataene som innhentes kan bli beriket med andre data som PST allerede har. Det fremgår ikke hvordan man tenker å plukke ut, filtrere, analysere og lagre relevant informasjon fra alle relevante deler av internett, med fortløpende endringer, og samtidig holde informasjonen mest mulig korrekt og representativ. PSTs formål med dataene skiller seg fra formålene som de individuelle datakildene har for dataene, og dataene vil bli gjenstand for blant annet utvalg og filtrering før PST lagrer dem. Denne behandlingen vil kunne gjøre at informasjonen tas ut av kontekst og ikke lenger er representativ. Et system som skal gjøre utdrag fra hele internett, vil nødvendigvis bare kunne lagre utdrag og «bruddstykker» av all relevant informasjon.

Dataforeningen uttaler at forslaget innebærer en generell og udifferensiert innhenting av åpen informasjon. Dette innebærer i praksis en masseovervåking av borgernes ytringer i det offentlige rom, som etter Dataforeningens syn ikke er et akseptabelt virkemiddel. Høringsnotatet inneholder svært begrensede begrunnelser for de behovene som beskrives, og det er derfor vanskelig å vurdere forholdsmessigheten av et slikt inngrep.

IKT-Norge mener at oppgaven som skal ivaretas og tilrettelegges for gjennom lovforslaget, fremstår som svært tynt begrunnet. Forslaget underbygges ikke verken med konkrete eksempler på situasjoner som kan avverges ved tiltaket, erfaringer fra andre land eller tilsvarende. IKT-Norge hadde forventet å se en begrunnelse for at tiltaket kan ha en faktisk effekt, som et minimumskrav for å akseptere inngrepet.

NITO mener at forslaget åpner for å registrere informasjon om enkeltpersoner, lagre denne, for så å kunne drive etterretning mot egne borgere i etterkant, noe som strider mot demokratiets prinsipper for innsamling av elektroniske spor. NITO frykter at en såpass massiv innsamling av informasjon vil kunne føre til svært mange ønsker om

sekundærbruk som ikke er forenelig med det opprinnelige formålet med tiltaket. En del av løsningen kan være å avgrense anvendelsen slik at innsamlede data anonymiseres fra starten av, før lagringen finner sted i PSTs systemer. Det er da viktig at anonymiseringen er reell, slik at det ikke er mulig å identifisere personer eller små grupper.

UTSYN mener det er grunn til å anta at oppdraget kan la seg løse på en måte som lar PST innhente informasjon fra åpne kilder i bulk, samtidig som innsamlingen begrenses til det som vil være relevant for formålet med innhentingen. Innhenting av informasjon i bulk fra åpne kilder vil måtte innrettes på ulike måter mot ulike trusselaktører og fenomener. Innhentingen kan begrenses ved at den for eksempel retter seg mot spesifikke nettsteder eller plattformer, eller at det defineres terskelverdier for hva som er å anse som en identifikator på budskap som kan knyttes opp mot for eksempel ekstremisme. Slike vurderinger vil uansett måtte gjøres av PST selv i forbindelse med innhenting og analyse av dataene, uavhengig av type trussel- og kriminalitetsfenomen. Man kan se for seg at PST tar utgangspunkt i en liste av nøkkelbegreper som identifiserer relevante nettsteder, og at hele eller deler av innholdet på de relevante nettstedene lagres. En slik liste kan revideres av interne og eksterne kontrollmekanismer, slik at det etableres en form for demokratisk kontroll over innhentingen samtidig som at PST gis forutsetninger til å løse sine lovpålagte oppgaver. Innretningen må understøttes av teknologiske løsninger, og hvilken teknologi som velges vil påvirke hva som er praktisk gjennomførbart. Lovteksten må utformes på en måte som muliggjør utvikling eller anskaffelse av informasjonssystemer og applikasjoner som understøtter behandlingen.

8.3.3 Departementets vurderinger

Departementet opprettholder at det er behov for at PST skal kunne benytte åpent tilgjengelig informasjon for å utarbeide analyser og etterretningsvurderinger om forhold i Norge som kan true nasjonale sikkerhetsinteresser. Når aktiviteten i stor grad foregår på nett, bør PST ha mulighetene og verktøyene til å kunne følge med den. Dette vil som beskrevet i høringsnotatet ikke være mulig uten at informasjonen kan lastes ned og analyseres nærmere. Etter departementets vurdering må det i en slik sammenheng også aksepteres at mye av informasjonen i seg selv er av liten eller ingen interesse for PSTs oppgaveløsning.

Departementet ser imidlertid at det er behov for å beskrive hva informasjonen er ment brukt til noe nærmere. Formålet med behandlingen er ikke individrettet, men å gi beslutningsstøtte, det vil si å danne grunnlag for taktiske, operasjonelle og strategiske beslutninger. Analyser og etterretningsvurderinger vil kunne bidra til å gi en retning og en prioritering for PSTs arbeid på ulike felter. Ved å kunne analysere omfanget av trusler på ulike områder vil PST i større grad kunne innrette sin innsats mot de områdene der det er nødvendig. Som eksempel kan nevnes at dersom analyse av åpent tilgjengelig informasjon tilsier at det foregår omfattende påvirkningsoperasjoner, er dette et område PST bør prioritere. Er omfanget av høyreekstreme uttalelser eller hets mot myndighetspersoner økende, kan PST måtte rette større oppmerksomhet mot disse feltene.

Videre vil vurderingene gi norske myndigheter verdifull informasjon om omfanget av ulike trusler i Norge i dag, samt potensielle trusler i fremtiden, slik at myndigheten kan innrette tiltak og ressurser mot dette. For eksempel kan omfang av strategiske oppkjøp eller russisk aktivitet i Norge være av betydning for hvilke tiltak som prioriteres. Det samme gjelder innenfor ulike sektorer der det er stort behov for å vite hvordan ulike trusselaktører opererer for å kunne forsvare seg mot uønskede hendelser, det være seg ulovlig etterretning, cyberangrep eller sabotasje.

Flere høringsinstanser er kritiske til at det ikke gjøres noen begrensninger på selve innsamlingen av informasjon, og peker på at målretting står sentralt i praksis fra EMD og EU-domstolen. I høringsnotatet la departementet til grunn at en avgrensning av innhentingen kunne være vanskelig å gjennomføre i praksis, og det ble ikke foreslått noen begrensninger i regelverket i hva som *kan* hentes inn.

Etter en fornyet vurdering har departementet imidlertid kommet til at det er ønskelig å ramme inn innhentingen til en viss grad. Dette vil bidra til å møte bekymringer for at PST kan lagre «hva som helst» helt uavhengig av om det har noen betydning for tjenestens oppgaver. Også for PSTs egen del er det ønskelig at informasjonen som behandles er mest mulig relevant for tjenestens oppgaveløsning, selv om den enkelte opplysning i seg selv ikke nødvendigvis er av interesse.

Grunnleggende for all etterretning er at den har til formål å danne grunnlag for beslutninger. Etterretningsprosessen er en styrt prosess, som utløses av at en beslutningstaker har et behov for økt kunnskap, for eksempel om fenomener som kan utgjøre en trussel. Dette behovet vil normalt

kunne dokumenteres. Informasjonsbehovet kan oppstå på ulike måter, enten det er at overordnet organ eller andre offentlige organer har behov for informasjon til støtte for sine beslutninger, eller at PST selv ser behov for å kartlegge en mulig trussel nærmere. Det kan være et planmessig ønske om eksempelvis å få oversikt over utvikling på et område, eller mer tilfeldig. Sistnevnte kan være dersom PST blir kjent med noe som kan være indikasjon på en mulig trussel, og det er ønskelig å finne ut om det er mer informasjon om denne på åpne kilder. Det kan også være aktuelt der et lekket datasett eller et nettsted antas å inneholde informasjon som kan være nødvendig for å utarbeide analyser og etterretningsvurderinger, og PST ønsker å laste dette ned for å kunne arbeide videre med materialet.

Som flere har pekt på vil PST selv måtte gjøre visse valg og avgrensninger når informasjonen skal lagres. En slik avgrensning kan gjøres på mange måter, eksempelvis ved at hele nettsteder som kan inneholde informasjon av interesse, lagres, at det først gjøres målrettede søk for å finne de aktuelle nettstedene, eller i form av nærmere undersøkelser etter mer tilfeldig funn av informasjon som det er grunn til å se nærmere på.

Samtidig kan mulighetene til å behandle informasjon etter den nye bestemmelsen ikke være for snever dersom virkemiddelet skal få den ønskede effekten. Vurderingen av hva som skal behandles må nødvendigvis være overordnet og kunne favne bredt. Det kan heller ikke kreves sikker kunnskap om at det for eksempel finnes informasjon av betydning for analyser og etterretningsvurderinger på et bestemt nettsted for at informasjon fra nettstedet kan lagres og analyseres. Det er behov for et bredt informasjonsgrunnlag dersom tjenesten skal kunne følge utvikling og trender i trusselbildet. For å kunne oppdage avvik eller en negativ utvikling, må PST ha nok informasjon til at tjenesten vet hva som er «normalsituasjonen». Det er heller ikke ønskelig å avgrense mot at PST for eksempel kan laste ned datasett for å undersøke om de inneholder opplysninger av etterretningsmessig verdi, selv om det ikke er direkte knyttet til et konkret informasjonsbehov på nedlastingstidspunktet. I slike tilfeller vil det være tilstrekkelig at datasettet antas å inneholde informasjon som kan være nødvendig for å utarbeide analyser og etterretningsvurderinger.

Regelverket må derfor formuleres på en måte som ikke innebærer en risiko for at PST går glipp av viktig og etterretningsrelevant informasjon, eller som gjør det mulig for trusselaktørene å forutse hvor PST vil rette oppmerksomheten og tilpasser sin virksomhet for å unngå å komme i PSTs søkelys. Hvordan PST skal avgrense innhentingen kan derfor ikke reguleres i detalj, men må konkretiseres i interne retningslinjer og rutiner.

Departementet foreslår etter dette som et vilkår for behandling etter bestemmelsen at behandlingen «må antas å være nødvendig» for utarbeidelse av analyser og etterretningsvurderinger. Kravet om at behandlingen må «antas» å være nødvendig, innebærer at det ikke kreves sannsynlighetsovervekt eller sikkerhet for at det vil være nødvendig å behandle opplysningene. Det vil være tilstrekkelig med at en rimelig og ikke helt fjern mulighet for at behandlingen er nødvendig. Dette er en følge av at PST etter departementets syn må kunne gå bredt ut for å finne informasjon av betydning for analyser og etterretningsvurderinger for å bidra til å sikre nasjonale sikkerhetsinteresser. I en slik situasjon må det aksepteres at tjenesten også behandler informasjon som det kan vise seg at er uten betydning for tjenestens oppgaveløsning.

Et krav om at behandlingen må antas å være nødvendig vil like fullt innebære en reell konkretisering av innhentingsadgangen. PST kan dermed ikke laste ned datasett, nettsteder eller lignende der det kun er en teoretisk eller fjern mulighet for at det kan finnes informasjon av etterretningsmessig verdi. Det er imidlertid ikke krav om at opplysningene *må* være nødvendige.

Etter departementets vurdering vil denne innrammingen av innhentingen av åpent tilgjengelig informasjon ytterligere understreke forskjellen mellom den behandlingen bestemmelsen her åpner for og E-tjenestens hjemmel for bulkinnhenting av kommunikasjon i transitt. Ved at innhentingen er betinget av at den antas nødvendig for utarbeidelse av analyser og etterretningsvurderinger, er innhentingen etter bestemmelsen mer begrenset og målrettet enn ved tilrettelagt innhenting. Dette gjør at forslaget i denne proposisjonen skiller seg fra systemene dommene fra EMD og EU-domstolen tok stilling til, og gjør at de krav som der er oppstilt har begrenset overføringsverdi til forslaget her.

En mer målrettet innhenting, kombinert med at informasjonen er offentlig tilgjengelig, gjør også at departementet ikke ser behov for en uavhengig forhåndskontroll med eller autorisasjon for innhentingen. Det anses tilstrekkelig at det foreligger interne rutiner hvor vilkårene for innhentingen fremgår og at det kan dokumenteres at innhentingen knytter seg til konkrete informasjonsbehov. Dette vil EOS-utvalget kunne kontrollere som ledd i sin alminnelige kontroll med tjenesten.

Når det gjelder valg av innhentingsmåte og tekniske løsninger for dette, legger lovforslaget ikke føringer for *hvordan* opplysningene teknisk hentes inn. Ut over at det etter denne bestemmelsen er snakk om større mengder informasjon, skiller innhentingen seg ikke fra innhenting av åpent tilgjengelig informasjon i andre sammenhenger. Det sentrale er at opplysningene er åpent tilgjengelig, slik at det ikke vil kunne behandles opplysninger etter bestemmelsen dersom de ikke er allment tilgjengelig for offentligheten på innhentingstidspunktet.

Når det gjelder den videre bruken av opplysninger i forbindelse med utarbeidelse av analyser og etterretningsvurderinger, ser departementet ikke behov for en forhåndskontroll med søk i opplysningene eller behandlingen for øvrig. I disse tilfellene behandles opplysningene for det formål de er innhentet for, og det bør derfor ikke begrenses hvordan denne behandlingen kan skje. Informasjonen som behandles etter forslaget er åpent tilgjengelig, og er dermed av en annen karakter enn informasjon som EMD-dommene dreier seg om. Åpen tilgjengelig informasjon vil også kunne søkes opp på nett så fremt informasjonen ikke er slettet, og det gjelder da ingen begrensninger i PSTs søkemuligheter. Det at PST har opplysningene lagret hos seg fremfor å måtte søke de opp på nett, er etter departementets vurdering ikke noe som tilsier at det må etableres forhåndskontroll for at PST skal kunne behandle opplysningene for det formål de er innhentet for. Eventuelle ytterligere krav for behandling til forebygging og etterforsking omtales nærmere i punkt 8.6 nedenfor.

Det er stilt spørsmål ved om dataene som innhentes kan berikes med andre data PST allerede har. Selv om informasjonen ligger atskilt fra PSTs øvrige registre, må PST likevel kunne se informasjonen i sammenheng med annen informasjon tjenesten besitter. Søk i opplysningene innenfor de oppstilte formålene vil kunne skje på bakgrunn av opplysninger PST allerede har registrert i sine alminnelige systemer. Videre vil de ferdige analysene og etterretningsvurderingene kunne inneholde opplysninger fra en rekke kilder, enten det er forskning, informasjon fra samarbeidende tjenester eller fra tidligere trusselvurderinger.

Departementet ser det på nåværende tidspunkt ikke som aktuelt å regulere innhenting av åpen tilgjengelig informasjon som en metode for politiet eller for PST. En slik bestemmelse er etter departementets syn heller ikke nødvendig. Åpne kilder er en av mange kilder for de opplysninger som allerede behandles av PST og politiet for øvrig. Politiregisterloven regulerer behandlingen også av disse opplysningene, ettersom loven ikke skiller på hvor opplysningene stammer fra. Opplysninger kan behandles så lenge lovens vilkår er oppfylt, uavhengig av om de stammer fra åpne kilder, andre offentlige organer, tips, kontakt med publikum eller andre kilder.

8.4 Unntak fra krav til opplysningenes kvalitet, behandling av særlige kategorier av personopplysninger mv.

8.4.1 Forslaget i høringsnotatet

Adgangen til å laste ned store mengder åpent tilgjengelig informasjon passer ikke inn i politiregisterlovens alminnelige regler om behandling av opplysninger. Det ble derfor foreslått å gjøre unntak fra kravene i politiregisterloven § 6, herunder kravene til at opplysningene som behandles skal være relevante og korrekte. Det ble vist til at når informasjon publiseres på internett vil PST ikke ha noen mulighet til å vurdere om den enkelte opplysning faktisk er korrekt.

I tillegg ble det vurdert å være behov for å gjøre unntak fra politiregisterloven § 7, som gir anvisning på at behandling av særlige kategorier av personopplysninger bare kan finne sted dersom det er strengt nødvendig ut fra formålet med behandlingen. Mange publiserer denne typen opplysninger på internett, eksempelvis om politisk eller religiøs overbevisning, seksuell orientering osv. I høringsnotatet ble det vist til at det ikke vil være mulig å filtrere ut slike opplysninger.

8.4.2 Høringsinstansenes syn

Riksadvokaten stiller spørsmål ved hvorvidt det er behov for generelle unntak fra §§ 6 og 7. Både relevanskravet og det strenge nødvendighetskravet for behandling av visse personopplysninger burde i prinsippet gjelde også ved masseinnhenting av informasjon, og så vidt riksadvokaten forstår er det i første rekke praktiske begrensninger som begrunner forslaget om unntak. I den grad det lar seg gjøre å sortere ut overskuddsinformasjon, enten i forbindelse med innhenting eller senere, antas det at lovens utgangspunkt burde være at denne muligheten i rimelig grad skal benyttes. Det kunne således vurderes å oppstille som vilkår for behandling av overskuddsinformasjon at utsortering og sletting ville være umulig eller uforholdsmessig ressurskrevende.

Datatilsynet viser til at det ikke er drøftet om en mer målrettet metode kunne ha oppfylt formålene. Målretting står helt sentralt både i praksis fra EMD og EU-domstolen. Datatilsynet understreker betydningen av korrekte opplysninger ved bruk av automatiserte analyseverktøy og eventuell bruk av kunstig intelligens, og den fare for algoritmeskjevhet (bias) det ellers kan medføre. Det må også tas med i betraktningen at noen publiserer sensitive opplysninger om andre mot deres vilje og på en ulovlig måte. Selv om opplysningene lagres ustrukturert, kan analyseverktøy raskt og enkelt kategorisere opplysningene.

Medietilsynet mener at innsamlingen av data om etnisitet, seksuell orientering, politisk tilhørighet, i tillegg til datainnsamling om mindreårige, i liten grad er problematisert i høringsnotatet.

Norges institusjon for menneskerettigheter (NIM) viser til at avgrensning mot lagring av sensitive personopplysninger ikke har annen begrunnelse enn at det ikke vil være mulig å skille ut disse opplysningene. NIM savner en mer grundig redegjørelse for betenkelighetene med en slik innsamling, både av hensyn til personvernet og av hensyn til ytringsfriheten. Videre savner NIM en omtale av om det kan innføres mekanismer for å unngå betenkelighetene ved å samle inn slike opplysninger. Det er eksempelvis ikke innført eller diskutert noen begrensninger knyttet til bruk av disse opplysningene.

Advokatforeningen har forståelse for at det er vanskelig å anvende prinsippene etter lovens §§ 6 og 7 for bulkinnsamling av data. Samtidig er de rettslige prinsippene som det gjøres unntak fra sentrale rettssikkerhetsprinsipper og ivaretar interesser som anses som sterkt beskyttelsesverdige, for eksempel fagforeningstilhørighet, politisk syn, etnisitet mv. Advokatforeningen mener at ulempene ved å bruke slike unntak burde vært vurdert.

Dataforeningen mener at det må etableres en mekanisme for kvalitetskontroll av den informasjonen som samles inn for å benyttes til analyse, og at mekanismene må være etterprøvbare. Det må etableres en kvalitetskontroll og kontroll av korrektheten i resultatet av analysene når resultatet skal benyttes, og rettssikkerhetsgarantier for at resultatet av analysevirksomheten skal kunne benyttes til å etablere konkret sak rettet mot enkeltpersoner eller grupper.

Tekna viser til at selv om det er krav om at informasjonen skal være en korrekt kopi av det PST har funnet på det åpne nettet, kan «korrekt kopi» av begrenset, utvalgt informasjon likevel gi et feil helhetsbilde. Det vises i den forbindelse til at åpen tilgjengelig informasjon også vil omfatte uriktig informasjon som er lagt ut av andre.

8.4.3 Departementets vurderinger

Departementet har merket seg at flere instanser uttrykker forståelse for at det vil være vanskelig å filtrere ut opplysninger som ikke er relevante eller særlige kategorier av personopplysninger ved innsamlingen av åpent tilgjengelig informasjon.

Flere av kravene som stilles i politiregisterloven § 6 vil ikke være mulig å oppfylle for den typen behandling forslaget her åpner for. Som det ble vist til i høringsnotatet er det ikke mulig å sikre at opplysninger i det sperrede materialet er korrekte og oppdaterte, eller at det ikke behandles flere opplysninger enn det som er nødvendig for å oppnå formålet. Angivelsen i § 6 fjerde ledd om at opplysninger i noen sammenhenger anses å være korrekte dersom de er gjengitt slik kilden ga dem, kan i og for seg være aktuell for opplysningene, ved at de vil behandles i den form de har fremkommet på den åpne kilden. Bestemmelsen er imidlertid utformet med tanke på andre situasjoner enn det som her er tilfelle, typisk referatsituasjoner som avhør av vitner mv.

For at PST skal kunne utarbeide analyser og etterretningsvurderinger om forhold i Norge som kan true nasjonale sikkerhetsinteresser, er det behov for et bredt informasjonsgrunnlag. Dersom PST skal se på utviklingen innenfor et område over tid, eksempelvis omfanget av høyreekstreme i Norge, må tjenesten ha nok informasjon til å kunne etablere en «normaltilstand» for å se om og i tilfelle hvordan denne endrer seg. For å avdekke om det foregår påvirkningsoperasjoner, er det nødvendig med informasjon om hva som er «vanlig» aktivitet i sosiale medier for å kunne identifisere eventuelle avvik. Som det ble beskrevet i høringsnotatet vil dette innebære at PST vil kunne behandle svært store mengder informasjon der mange av opplysningene er av liten eller ingen interesse for PSTs virksomhet.

Det er mange som publiserer særlige kategorier av personopplysninger om seg selv eller andre. Opplysningene vil kunne fremkomme i mange ulike former, eksempelvis i en løpende diskusjon på et chan-fora, eller i fritekst på en nettside som ellers kan tenkes å inneholde informasjon av betydning for utarbeidelse av analyser og etterretningsvurderinger. Å filtrere ut disse opplysningene ved innsamlingen, uavhengig av i hvilken form de fremkommer, vil ikke være mulig. Selv om dette betyr at opplysninger for eksempel om en persons seksuelle legning kan tenkes å fin-

nes i det innhentede materialet uten at opplysningene er strengt nødvendig for å utarbeide analyser og etterretningsvurderinger, mener departementet at dette må aksepteres. Opplysningen er uansett åpent tilgjengelig. Den tilleggsulempen PSTs behandling innebærer for den enkelte, reduseres ved at opplysningene vil være sperret, jf. omtalen i punkt 8.5 nedenfor, og derfor kun kan behandles for særskilt angitte formål. I andre sammenhenger anses opplysningene ikke å være registrert hos PST.

Departementet opprettholder derfor at det er behov for å gjøre unntak fra kravene etter §§ 6 og 7. Imidlertid foreslås det å gjøre unntakene mer begrenset enn i høringsnotatet. Det er først og fremst ved innhentingen og lagringen at behovet for unntak fra bestemmelsene gjør seg gjeldende. Når det ikke stilles krav om at PST på forhånd må ha sikker kunnskap om at et nettsted, datasett eller lignende inneholder opplysninger som er nødvendige for analyser og etterretningsvurderinger, kan det heller ikke stilles krav om at opplysninger som er irrelevante eller gjelder særlige kategorier av personopplysninger ikke samles inn eller lagres.

I tillegg er det behov for å opprettholde unntakene når opplysningene behandles ved hjelp av automatiserte analyseverktøy. Slike verktøy skal blant annet kunne brukes til å kartlegge trender og utviklingstrekk og gi prediksjoner om forventet utvikling. Denne typen automatiserte analyser krever et bredt informasjonsgrunnlag for å kunne gi mest mulig presise resultater. Automatiserte analyseverktøy må derfor kunne benyttes på alle de innhentede opplysningene, uavhengig av om den enkelte opplysning er relevant og oppdatert eller om det kan finnes særlige kategorier av personopplysninger i materialet.

Unntakene fra kravene etter §§ 6 og 7 vil etter dette kun gjelde for innhenting, lagring og bruk av automatiserte analyseverktøy. For all annen behandling i forbindelse med utarbeidelse av analyser og etterretningsvurderinger vil kravene gjelde fullt ut. Heller ikke ved bruk i forebyggende sak eller til etterforsking gjøres det noen unntak fra kravene. Behandling av eventuelle særlige kategorier av opplysninger i en analyse eller etterretningsvurdering, en forebyggende sak og i etterforsking må derfor være strengt nødvendig, og opplysningene må være relevante, korrekte og oppdaterte.

Riksadvokaten har foreslått å oppstille som vilkår for behandling av overskuddsinformasjon at utsortering og sletting ville være umulig eller uforholdsmessig ressurskrevende. Departementet mener at en utsortering og sletting av overskuddsinformasjon gjennomgående vil være tilnærmet umulig eller uforholdsmessig ressurskrevende, og at det er vanskelig å begrense hva som lagres ut over den målrettingen av innhentingen som er beskrevet i punkt 8.3.3 ovenfor. En mer målrettet innhenting vil gjøre at mengden irrelevant informasjon er mindre. Dersom PST etter å ha analysert for eksempel et datasett finner at det er uten betydning for utarbeidelse av analyser og etterretningsvurderinger, skal informasjonen slettes, jf. omtalen i punkt 8.8.3. Det samme vil gjelde dersom deler av materialet er uten betydning, gitt at det er mulig å skille de relevante og irrelevante delene fra hverandre.

8.5 Sperring

8.5.1 Forslaget i høringsnotatet

I høringsnotatet ble det vist til at de personvernmessige betenkelighetene ved ordningen må kompenseres så langt det lar seg gjøre, herunder gjennom etablering av tilstrekkelige sikkerhetsmekanismer for å unngå misbruk.

For å begrense følgene for den enkelte i størst mulig grad, foreslo departementet at opplysningene i sin helhet skal sperres. Den mest sentrale konsekvensen av sperring er at sperrede opplysninger ikke anses for å være «registrert» i politiregisterlovens forstand. Dette gjør at opplysningene ikke kan brukes som ledd i den virksomheten registrerte opplysninger vanligvis brukes til. PST kan derfor ikke søke i disse opplysningene i forbindelse med for eksempel sikkerhetsklareringer, henvendelser fra andre organer eller andre løpende oppgaver. Opplysninger som er sperret vil heller ikke kunne utleveres til andre. Dersom opplysningene skal kunne brukes til andre formål enn etterretningsvirksomhet, må dette reguleres særskilt.

8.5.2 Høringsinstansenes syn

Forsvarsdepartementet ber om at det presiseres hva som menes med at opplysningene ikke vil kunne utleveres til andre. Det er Forsvarsdepartementets syn at evaluerte data skal kunne utleveres etter de generelle reglene om utlevering i politiregisterloven kapittel 6, selv om de er innhentet i bulk.

Politidirektoratet og *Kripos* mener det ikke er nødvendig – og heller ikke riktig – å gjøre bruk av begrepet sperring når bestemmelsen uansett entydig avgrenser hvilke formål opplysningene

skal kunne brukes til, og at de skal slettes etter en viss tid.

De lagrede opplysningene kan brukes i PSTs etterretningsvirksomhet, samt at det kan foretas søk i opplysningene for å opprette forebyggingssak, i forebyggingssak og i etterforskningsøyemed, dvs. i praksis innenfor stort sett hele PSTs ansvarsområde. Det blir således noe misvisende at overskriften i § 65 a har overskriften «Behandling av åpent tilgjengelig informasjon til etterretningsformål». Dersom de lagrede opplysningene benyttes for forebygging og etterforsking, kan PST registrere opplysningene i sine alminnelige registre. Det kan derfor stilles spørsmål ved sperringens funksjon som sikkerhetsmekanisme.

Oslo statsadvokatembeter, Politidirektoratet og *Kripos* peker på at i gitte tilfeller vil PST ha en plikt til å videreformidle informasjon til det øvrige politi, jf. plikten etter straffeloven § 196 til å avverge straffbare forhold. PST kan også ha plikt til å gi opplysninger til andre. For Kripos fremstår det som helt klart at det behandlingsformål og de bruksbegrensninger som angis i § 65 a ikke fritar PST for å vurdere sin aktivitetsplikt etter annen lovgivning, herunder straffeloven § 196 og § 226, samt barnevernloven § 6-4.

Riksadvokaten støtter i utgangspunktet forslaget om at åpent tilgjengelig informasjon som innhentes til formål som angitt i høringsnotatet, skal sperres. Fordi utkastet til endring i politiloven § 17 b ikke sondrer mellom etterretningsopplysninger innhentet til ulike formål, kan det imidlertid fremstå uklart om sperreplikten også vil gjelde der etterretningsopplysninger er innhentet som ledd i etterforsking.

Stortingets kontrollutvalg for etterretnings-, overvåkings- og sikkerhetstjeneste (EOS-utvalget) mener det i utgangspunktet er positivt at opplysninger fra masseinnsamlingen via åpne kilder holdes adskilt fra annen informasjon som PST lagrer, og at det oppstilles klare adgangsbegrensninger. Selv om dette ikke er «registrering» i politiregisterlovens forstand, innebærer imidlertid også en slik sperret behandling en lagring av personopplysninger som bør være omsluttet av klare regler.

Utvalget påpeker at det ved innføring av en ny metode der sperring utgjør en sentral del av reguleringen, er viktig at adekvat sperrefunksjonalitet er på plass i PSTs systemer før innhenting settes i gang. EOS-utvalget må kunne kontrollere sperrefunksjonaliteten. Det er nødvendig at PST tilrettelegger sine systemer for kontroll, ved å bygge inn kontrollmuligheter. Dette bør gjøres i samråd med utvalget, for å sikre at kontrollbehovene ivaretas.

Sperring vil etter *Norges institusjon for menneskerettigheters (NIMs)* syn bidra til å sikre at opplysningene holdes atskilt og ikke benyttes i større utstrekning enn loven gir anvisning på. Samtidig gir loven en svært vid adgang til å innsamle og benytte opplysningene, og lite begrensninger på hvilke personer som kan få tilgang til dem. Dette reduserer vekten av sperring som et egnet sikkerhetstiltak.

Datatilsynet kan ikke se at de foreslåtte reglene innebærer noen reelle eller praktiske begrensninger for PSTs bruk av opplysningene. Spesielt ved bruk til forebygging og etterforsking vil søk være rettet mot enkeltpersoner, uten at det legges opp til en uavhengig forhåndskontroll.

Advokatforeningen støtter forslaget om at opplysningene i sin helhet skal sperres, slik at opplysningene ikke kan søkes i eller benyttes for andre formål eller deles med andre.

Tekna viser til at det at opplysningene skal «sperres», slik at kun personer med særskilt bemyndigelse skal få adgang, er omtalt som en sentral sikkerhetsmekanisme. Tekna savner en nærmere vurdering av om denne sikkerhetsmekanismen er tilstrekkelig. Det er en fare for formålsutglidning, slik at data, inkludert analyser og andre sammenstilte data, på sikt vil brukes på en annen måte enn det som er tenkt i dag.

8.5.3 Departementets vurderinger

De fleste høringsinstansene som har uttalt seg om spørsmålet, støtter forslaget om at opplysningene skal sperres. På bakgrunn av at både Politidirektoratet og Kripos mener at det ikke er nødvendig, og heller ikke riktig, å gjøre bruk av begrepet sperring når bestemmelsen uansett entydig avgrenser hvilke formål opplysningene skal kunne brukes til, redegjøres det likevel nærmere for hvorfor opplysningene etter forslaget skal være sperret.

Som det fremgår av punkt 4.2 innebærer sperring at den fremtidige behandlingen av opplysninger begrenses, samt at det ved sperring alltid må oppgis hvilke formål sperrede opplysninger kan brukes til. Formålsbegrensning kan oppnås også uten å benytte seg av sperreinstituttet, ved at det reguleres hvilke formål de registrerte opplysningene kan brukes til. Sperring innebærer normalt at politiet har behandlet opplysningene før de sperres, jf. politiregisterloven § 2. nr. 10 om at hensikten med sperring er å begrense den «fremtidige» behandlingen. Samtidig finnes det enkelte regler i politiregisterforskriften der sperring skal benyttes også før opplysningene er behandlet. Eksempelvis følger det av politiregisterforskriften

§ 59-11 at opplysninger i registeret for Nasjonalt tverretatlig etterretningssenter (NTAES) skal sperres for å sikre at de bare kan benyttes i NTAES til registerets formål.

Sperring har også andre konsekvenser enn at det begrenses hvilke formål opplysningene kan brukes til. Den fremste grunnen til at det foreslås at opplysningene skal være sperret er at de da i politiregisterlovens forstand ikke anses for å være registrert. Dette fremgår ikke eksplisitt av politiregisterloven, men er forutsatt i forarbeidene til loven, jf. Ot.prp. nr. 108 (2008–2009) punkt 21.7 side 314.

Dersom opplysningene ikke sperres, er konsekvensen at de lagrede opplysningene vil utgjøre et register på lik linje med politiets øvrige registre, med den følge at alle personer som figurerer i det lagrede materialet også er «registrert» hos PST. Hovedhensikten med politiets øvrige registre er at det behandles opplysninger om enkeltpersoner til de formål som er angitt i regelverket. Dette er ikke hensikten med lagringen etter forslaget her. Tvert imot er lagringen av opplysninger om enkeltpersoner her en ulempe man må ta på kjøpet for å gi PST de nødvendige verktøyene for at de kan utføre sitt samfunnsoppdrag. På grunn av inngrepets art er det svært viktig å beskytte opplysningene på best mulig måte, samt å etablere en klar forskjell til politiets øvrige registre. Begge målsettingene oppnås best ved at opplysningene i sin helhet er sperret.

Enkelte høringsinstanser har stilt spørsmål ved om opplysningene kan utleveres til andre. I forslaget til § 65 a annet ledd er det gitt en uttømmende opplisting over de formålene opplysningene kan brukes til. Samtlige av formålene de sperrede opplysningene kan brukes til gjelder PSTs virksomhet. Så lenge opplysningene er sperret kan de ikke brukes til andre formål enn de oppgitte, og derved heller ikke utleveres til andre. Dette gjør at de sperrede opplysningene ikke vil kunne utleveres som følge av opplysningsplikt i annen lovgivning eller etter avvergingsplikten i straffeloven § 196. Imidlertid vil de samme opplysningene ligge åpent tilgjengelig på nett, med mindre de har blitt slettet fra det åpne nettet etter det tidspunktet PST lagret dem. Dersom PST kommer over opplysninger i det sperrede materialet som normalt ville blitt utlevert etter regler om opplysningsplikt eller avvergingsplikt, er det ingenting i veien for at PST undersøker om disse fremdeles finnes åpent tilgjengelig på nett. Gjør de det, kan PST varsle aktuell mottaker om opplysningene uten at de utleveres fra det sperrede materialet.

Opplysningene vil kunne utleveres til andre i form av analyser og etterretningsvurderinger, det vil si når de er bearbeidet og funnet relevante for etterretningsformål. Det samme gjelder for opplysninger som er tatt i bruk og flyttet over i PSTs vanlige registre, enten det er til forebyggende sak eller i etterforsking. Opplysningene vil i slike tilfeller ikke lenger være sperret, og vil behandles, herunder kan de utleveres, etter de vanlige reglene i politiregisterloven. Opplysninger som er sperret og ikke tatt i bruk vil derimot ikke kunne utleveres. Ettersom denne begrensningen ikke fremkommer eksplisitt i dagens regler om sperring, tar departementet sikte på å regulere dette i forskrift.

8.6 Bruk til forebyggende sak og etterforsking

8.6.1 Forslaget i høringsnotatet

Selv om formålet med behandlingen er ivaretakelse av PSTs etterretningsvirksomhet, ble det foreslått at de sperrede opplysningene også kan brukes i de tilfellene der det er åpnet etterforsking eller opprettet forebyggende sak, samt for åpning av etterforsking eller opprettelse av forebyggende sak. Det ble vist til at hvis det i de sperrede opplysningene finnes informasjon om personer som PST allerede har i søkelyset, eller om personer som utgjør en reell trussel, bør PST kunne behandle denne informasjonen.

Når PST først har gått til det skritt å opprette en forebyggende sak, søker tjenesten å forebygge alvorlige straffbare handlinger. Dersom PST allerede har en forebyggende sak, vil de etter forslaget derfor kunne søke i det sperrede materialet for å finne informasjon som har saklig tilknytning til den forebyggende saken. Adgangen til å søke i det sperrede materialet ble også foreslått å gjelde dersom opplysningene skal brukes til å *opprette* forebyggende sak. Dette innebærer eksempelvis at dersom PST, når de bruker opplysninger for etterretningsformål, kommer over opplysninger om en person som det er grunn til å undersøke om forbereder et straffbart forhold som PST skal forebygge, vil de kunne registrere denne personen i sine alminnelige registre. Det samme vil gjelde dersom PST får tips om en person det er knyttet en bekymring til, og de avdekker opplysninger som kan danne grunnlag for en forebyggende sak ved et søk i det sperrede materialet.

Når det gjelder bruk til etterforsking, ble det ikke foreslått ytterligere begrensninger enn at det må dreie seg om etterforsking av lovbrudd som

nevnt i politiloven § 17 b. PST er gitt i oppgave å etterforske svært alvorlige lovbrudd. Dersom det først er rimelig grunn til å undersøke om det foreligger et straffbart forhold av denne art, mente departementet at PST må kunne søke i de sperrede opplysningene for å klarlegge om det finnes opplysninger der av betydning for straffesaken.

Både forebygging og etterforsking av de straffbare handlinger som er nevnt i politiloven § 17 b har nær sammenheng med PSTs etterretningsmandat. Departementet anså derfor ikke slik bruk for å være en formålsutglidning. Det ble vist til at PST allerede i dag har mulighet til å benytte åpent tilgjengelig informasjon i forbindelse med forebygging og etterforsking. Det ble også vist til at PST kan benytte skjulte tvangsmidler både i etterforskingssporet og i det forebyggende sporet, noe som er langt mer inngripende enn den behandlingen forslaget her åpner for. På denne bakgrunn ville det etter departementets syn fortone seg som lite logisk å stenge for tilgang til informasjon som er offentlig tilgjengelig eller som har vært offentlig tilgjengelig i disse tilfellene.

Ved bruk til forebygging og etterforsking vil søk være rettet mot enkeltpersoner, og en slik bruk vil kunne være mer inngripende for personene det søkes etter. I høringsnotatet ble det uttalt at departementet hadde vurdert om det burde oppstilles ytterligere vilkår for bruk av de sperrede opplysningene for disse formålene, herunder om det burde stilles krav om en forutgående kontroll. Det ble vist til at departementet ikke var kjent med eksempler på ordninger hvor det oppstilles krav om domstolskontroll ved bruk av opplysninger det allerede er lovlig grunnlag for å behandle, og at et slikt krav etter departementets syn ikke kan utledes av EMDs praksis. Det ble derfor lagt til grunn at det ikke burde stilles krav om forutgående kontroll for søk til disse formålene.

8.6.2 Høringsinstansenes syn

Riksadvokaten og *Oslo statsadvokatembeter* er kritiske til at opplysningene bare skal kunne benyttes til etterforsking av lovbrudd som nevnt i politiloven § 17 b. *Det nasjonale statsadvokatembetet* understreker viktigheten av at den innhentede informasjonen kan brukes i etterforskingssak.

Oslo statsadvokatembeter mener at opplysningene generelt bør kunne brukes til etterforsking. PST bør kunne videreformidle innhentet åpent tilgjengelig informasjon til det ordinære politi og til påtalemyndigheten med ansvar for strafforfølgning av andre lovbrudd enn de som etterforskes av PST. *Riksadvokaten* mener at dersom departementet ikke finner grunn til fullt ut å åpne for bruk i etterforskingsøyemed, kan muligens en løsning etter modell av straffeprosessloven § 216 i om bruk av overskuddsinformasjon fra kommunikasjonskontroll, særlig bokstavene d til f, være tjenlig.

Stortingets kontrollutvalg for etterretnings-, overvåkings- og sikkerhetstjeneste (EOS-utvalget) bemerker at selv om det i overskriften til bestemmelsen bare blir nevnt «etterretningsformål», fremgår det at den innsamlede informasjonen også kan benyttes til å opprette en forebyggende sak eller til etterforskingsformål. Med en slik generell åpning for overføring til andre formål tjener allerede innsamlingen egentlig alle de tre formålene som PST skal ivareta. Dermed er hele innsamlingssystemet også et langt mer kraftfullt verktøy for PST, og dermed et potensielt langt større personverninngrep, enn overskriften til bestemmelsen kan gi inntrykk av. *Politidirektoratet* og *Kripos* har lignende synspunkter.

En utvisking av skillet mellom politi- og etterretningsvirksomhet for PSTs del har etter *EOS-utvalgets* syn prinsipielle, rettslige og faktiske konsekvenser. Sett fra et kontrollperspektiv kunne dette med fordel ha vært utredet nærmere. Bruk av opplysninger fra masseinnsamlingen i konkrete forebyggende saker og etterforsking vil utgjøre et nytt og kraftigere inngrep i de berørtes personvern og privatliv. Hvis tankegangen fra de nyeste EMD-dommene legges til grunn, bør det på dette stadiet legges inn ytterligere rettssikkerhetsgarantier. Også hensynet til utvalgets kontroll taler for at det defineres hva «bruk» av opplysninger som er innhentet for etterretningsformål i forebyggende sak innebærer, og på hvilke vilkår personopplysninger kan flyte mellom disse sporene.

Norges institusjon for menneskerettigheter (NIM) viser til at opplysningene i realiteten kan benyttes til samtlige av PSTs ansvarsområder. Dette gir en svært vid adgang til bruk av opplysningene, uten reell avgrensning, og uten forutgående kontroll. Etter NIMs oppfatning gir en såpass vid adgang til bruk av opplysningene grunn til å anse inngrepet som langt mer omfattende enn dersom formålet kun var å kartlegge trender og «følge med på internett». NIM forutsetter at vilkårene i politiregisterloven § 64 første ledd bokstav a må være oppfylt ved søk i materialet dersom man ønsker å undersøke om forebyggende sak overhodet skal opprettes, og at søkene som utføres må stå i saklig sammenheng med det som danner grunnlaget for

å utføre undersøkelsen. At søket må ha en slik saklig sammenheng kan med fordel presiseres i lovteksten.

NIM savner en bredere og mer prinsipiell diskusjon om adgangen er nødvendig opp mot hvert av de tre formålene, hvordan disse samlet sett påvirker inngrepsgraden, og i hvilken grad disse formålene gir borgeren tilstrekkelig beskyttelse for at opplysningene ikke benyttes utover det som er strengt nødvendig.

Departementet burde videre understreket tydeligere hvordan PST skal unngå at søk i materialet blir tilfeldig, gitt at formålet er såpass vidt. Dette har også en klar side til å unngå misbruk og formålsutglidning. En tydeligere avgrensning vil også gi borgerne mulighet til å forutse når opplysningene kan hentes ut. Endelig er en tydeligere avgrensning en forutsetning for at kontrollorganer skal kunne føre en meningsfull kontroll med hva som er lovlig lagring og bruk, og hva som ikke er det.

Datatilsynet kan ikke se at de foreslåtte reglene innebærer noen reelle eller praktiske begrensninger for PSTs bruk av opplysningene. Spesielt ved bruk til forebygging og etterforsking vil søk være rettet mot enkeltpersoner, uten at det legges opp til en uavhengig forhåndskontroll.

Medietilsynet mener det er stor forskjell på et formål om bedre risikoanalyser og på å bruke denne informasjonen til å overvåke enkeltpersoner. Det er behov for en tydelig formålsbegrensning, og en begrunnelse i lys av hvilke formål regelverksendringene åpner for. Medietilsynets tolkning er at de innsamlede dataene kan brukes til alle de tre delene av PSTs oppdrag, etterretning, forebygging og etterforsking, kun begrenset av sperring og adgangskontroll. Slik sett tar forslaget til orde for en omfattende overvåking, som stiller strengere krav til en begrunnelse enn det høringsnotatet legger opp til. Medietilsynet mener departementet bør klargjøre hvilket eller hvilke av PSTs formål innsamling og bruk av data er en del av, og begrunne inngrepene i ytringsfriheten på dette grunnlaget.

Advokatforeningen er ikke enig i forslaget om at de sperrede opplysningene uten videre også skal kunne brukes i de tilfellene der det er åpnet etterforsking av lovbrudd som nevnt i politiloven § 17 b eller i forbindelse med en forebyggende sak. I disse tilfellene har PST andre og mer målrettede virkemidler til rådighet. Bruk av masseinnhentet informasjon kan også stilles seg forskjellig avhengig av om det er snakk om bruk som grunnlag for å åpne en straffesak eller bruk i en pågående straffesak. I tillegg er de straffbare forholdene som er opplistet i politiloven § 17 b svært ulikeartet. Dersom opplysningene skal kunne brukes til andre formål enn etterretningsvirksomhet, må dette etter Advokatforeningens syn vurderes nærmere på prinsipielt grunnlag og det må også vurderes eksplisitt og særskilt for de ulike straffbare forholdene opplistet i politiloven § 17 b.

Tekna savner en utredning av konsekvensene av at PST kan bruke innsamlet informasjon til både etterretning, forebygging og etterforsking.

Dataforeningen mener at det bør etableres klare kriteria for en uavhengig forhåndskontroll av adgangen til å gjøre søk mot enkeltpersoner og bruk av innsamlede opplysninger i etterforsking av konkrete saker som faller inn under PST sitt ansvarsområde.

8.6.3 Departementets vurderinger

Departementet har merket seg at en rekke instanser mener at muligheten for at PST kan bruke opplysningene til forebyggende sak og etterforsking uthuler effekten av sperringen. Departementet vil derfor understreke at inngangsvilkåret for å behandle opplysningene er at det antas å være nødvendig for utarbeidelse av analyser og etterretningsvurderinger, jf. omtalen i punkt 8.3.3 ovenfor. Dette gjør at PST ikke kan *innhente* åpent tilgjengelig informasjon, uten at vilkårene i §§ 6 og 7 er oppfylt, til andre formål enn utarbeidelse av analyser og etterretningsvurderinger. Innhenting etter bestemmelsen med det formål å drive forebygging eller etterforsking er derfor avskåret. Departementet finner også grunn til å minne om at PST allerede i dag har full anledning til å behandle opplysninger som stammer fra åpne kilder til alle sine oppgaver, så fremt vilkårene for å behandle opplysningene er oppfylt, det vil blant annet si at de er nødvendige, formålsbestemte og relevante.

Hovedformålet med og inngangen for å kunne behandle opplysninger etter den foreslåtte bestemmelsen er behovet for opplysningene ved utarbeidelse av analyser og etterretningsvurderinger. Enkelte høringsinstanser synes å mene at øvrig bruk bør avskjæres eller begrenses i større grad enn det som ble foreslått i høringsnotatet. Departementet er ikke enig i dette, og ser det som svært uheldig dersom PST ikke skulle ha muligheten til å kunne bruke opplysninger de har lagret etter den nye bestemmelsen til etterforsking og forebyggende sak. Departementet mener heller ikke at det er behov for å innføre ytterligere sikkerhetsmekanismer for bruk til disse formålene, ut over mekanismene som allerede finnes i regel-

verket. Merverdien av å kunne bruke de sperrede opplysningene sammenlignet med søk på internett er at PST vil kunne finne og nyttiggjøre seg av opplysninger som er slettet på det åpne nettet. Opplysninger som fremdeles er åpent tilgjengelige vil PST fritt kunne søke opp og lagre uten at de hentes fra de sperrede opplysningene. Departementet mener derfor at søk i det sperrede materialet sammenlignet med søk på det åpne nettet vil være et begrenset ytterligere inngrep overfor den enkelte.

Samtidig finner departementet grunn til å minne om at bruk både til etterforsking og forebyggende sak innebærer at en del vilkår må være oppfylt. Forslaget her innebærer ingen unntak fra disse vilkårene. Etterforsking kan etter straffeprosessloven § 224 foretas når det som følge av anmeldelse eller andre omstendigheter er rimelig grunn til å undersøke om det foreligger straffbart forhold som forfølges av det offentlige. Etterforsking besluttes av påtalemyndigheten, jf. straffeprosessloven § 225. I den enkelte straffesak følger adgangen til å behandle opplysninger reglene i straffeprosessloven, jf. politiregisterloven § 64 annet ledd.

Inngangsvilkåret for å opprette en forebyggende sak er som nevnt i punkt 4.2 at det er grunn til å undersøke om noen forbereder et straffbart forhold som PST har til oppgave å forebygge. De forebyggende sakene er grundig regulert i politiregisterforskriften § 21-5. Sjef PST eller den han bemyndiger skal godkjenne opprettelsen, det kan bare behandles opplysninger som har saklig tilknytning til saken, og saken skal gjennomgås hvert år for vurdering av om den skal avsluttes eller videreføres. Departementet anser det derfor ikke nødvendig å innføre ytterligere krav eller rettssikkerhetsmekanismer for at opplysningene skal kunne brukes til dette formålet. Departementet finner igjen grunn til å understreke at personer som ytrer seg på en slik måte på nett at det er grunn til å undersøke om de forbereder et straffbart forhold innenfor PSTs mandat, uavhengig av dette forslaget vil kunne registreres, og opplysninger som finnes åpent tilgjengelig vil allerede i dag kunne brukes for å opprette en forebyggende sak.

De lovbrudd PST har i oppgave å forebygge og etterforske, er alle svært alvorlige og kan ha et betydelig skadepotensial for samfunnet. Departementet ser det derfor ikke som en aktuell løsning å begrense bruken til bare noen av de lovbruddene som er listet opp i politiloven § 17 b. Samtidig er det heller ikke grunn til å utvide adgangen til bruk til etterforsking av lovbrudd utenfor PSTs mandat, eller til andre formål enn de som er nevnt. Det er ikke unikt at PST har opplysninger som ikke kan deles med andre. Eksempelvis legger politiloven § 17 f begrensninger på hvilke formål opplysninger som er innhentet ved forebyggende tvangsmiddelbruk kan benyttes til. Også for opplysninger som PST har mottatt fra samarbeidende tjenester vil det kunne være begrensninger i adgangen til å utlevere opplysningene til andre. Det understrekes at dersom opplysningene først er tatt i bruk i en etterforsking, vil de alminnelige reglene i straffeprosessloven gjelde, eksempelvis reglene om dokumentinnsyn i straffeprosessloven § 242. Opplysningene vil dermed kunne inngå i sakens dokumenter og brukes som bevis i en eventuell straffesak.

Også der opplysningene tas i bruk i en forebyggende sak, vil de alminnelige reglene gjelde for videre behandling av opplysningene. Når opplysningene tas i bruk, vil de måtte flyttes over i PSTs vanlige registre, og de vil da ikke lenger være sperret. Som omtalt i punkt 8.4.3 gjelder ikke unntakene fra §§ 6 og 7 for bruk av opplysninger i forebyggende sak eller i etterforsking, slik at opplysningene blant annet må være korrekte og oppdaterte, og behandling av særlige kategorier av personopplysninger må være strengt nødvendig.

En rekke instanser har stilt spørsmål ved adgangen til å bruke opplysningene til *opprettelse* av forebyggende sak, særlig i kombinasjon med muligheten til å benytte automatiserte analyseverktøy. Som omtalt i punkt 8.9.3. åpnes det ikke for at automatiserte analyseverktøy kan brukes for å finne personer som det kan være aktuelt å opprette forebyggende sak på. At PST kan bruke slike verktøy i forbindelse med utarbeidelse av analyser og etterretningsvurderinger er derfor ikke et argument mot at PST skal kunne bruke opplysningene til å opprette forebyggende sak, dersom opplysningene først er av den karakter at de gir grunn til å opprette en slik sak.

Når innhentingen rammes inn, jf. punkt 8.3.3 ovenfor, vil informasjonen som hentes inn i større grad være rettet mot nettsteder mv. der det kan tenkes å være informasjon av betydning for analyser og etterretningsvurderinger. PST vil dermed ikke kunne samle inn all informasjon som finnes åpent tilgjengelig. Det foreslås også en atskillig kortere lagringstid, jf. punkt 8.8.3 nedenfor, noe som gjør at faren for at informasjonen er gammel og utdatert er mindre. Dette gjør samlet sett at departementet mener at det ikke bør legges begrensninger på PSTs muligheter til å benytte opplysningene til å opprette forebyggende sak.

Dersom det finnes opplysninger i det sperrede materialet som kunne bidratt til å forebygge for eksempel en terrorhandling, ville det vært utenkelig å pålegge PST å se bort fra disse opplysningene. Dette må gjelde selv om personen opplysningene gjelder ikke tidligere har vært i PSTs søkelys. Også der det kommer inn tips på en person som gir grunn til bekymring, bør man kunne forvente at PST forsøker å avdekke all relevant informasjon om personen for enten å bekrefte eller ta ned bekymringen.

Departementet opprettholder etter dette at de sperrede opplysningene skal kunne brukes i etterforsking av lovbrudd som nevnt i politiloven § 17 b, og til opprettelse av eller i en forebyggende sak, og at det ikke oppstilles ytterligere krav for å kunne bruke opplysningene til disse formålene enn de som allerede finnes i regelverket. Departementet understreker samtidig viktigheten av å sikre notoritet og kontroll med bruken av opplysningene. Dersom opplysninger tas ut av det sperrede materialet og benyttes i en forebyggende sak eller i etterforsking, skal det derfor fremgå klart av saken hvilke opplysninger som er hentet fra det sperrede materialet. Dette vil EOS-utvalget kunne kontrollere ved deres alminnelige kontroll med PSTs etterforskingssaker og forebyggende saker, jf. EOS-kontrolloven § 6 fjerde ledd nr. 1. På samme måte skal det fremgå klart dersom en sak er opprettet på bakgrunn av opplysninger som er hentet fra det sperrede materialet.

8.7 Kontrollmekanismer

8.7.1 Forslaget i høringsnotatet

I høringsnotatet ble det foreslått enkelte forskriftsregler om saksbehandling og kontroll, herunder krav om at tilgang bare skal gis til bemyndigede personer, og at all bruk av opplysningene skal kunne spores. Det ble ikke foreslått egne, detaljerte regler for behandling etter den nye bestemmelsen. Grunnen til dette er at det i politiregisterloven og politiregisterforskriften allerede er en rekke regler som vil komme til anvendelse for behandlingen, selv om de ikke nevnes særskilt. Departementet la til grunn at særskilte regler om lagring av opplysningene, begrensinger i bruken og etterfølgende kontroll, sett i sammenheng med politiregisterlovgivningens alminnelige regler om informasjonssikkerhet, internkontroll og sporing, ville ivareta de nødvendige kravene til sikkerhetsmekanismer.

I høringsnotatet ble det vist til at EOS-utvalgets kontroll vil være en viktig sikkerhetsmekanisme, og at kontroll med hvem som har tilgang til de sperrede opplysningene og kontroll med at søk i opplysningene kun skjer for de formålene loven åpner for vil være en naturlig del av EOS-utvalgets kontroll med tjenesten.

Det ble ikke foreslått å åpne for innsyn i opplysninger som behandles etter den nye bestemmelsen, både fordi det ville kunne innebære en risiko for at det avsløres hvilke områder på nettet PST velger å laste ned informasjon fra, og fordi merverdien av innsyn ville være begrenset, all den tid den enkelte fritt kan søke opp informasjon som er publisert på internett om en selv, og det ikke er aktuelt å føre kontroll med opplysningenes riktighet.

8.7.2 Høringsinstansenes syn

Politiets sikkerhetstjeneste (PST) støtter rettsikkerhetsmekanismene i forslaget, og finner at disse på en god måte vil balansere inngrepene i privatliv og ytringsfrihet.

Riksadvokaten mener at de foreslåtte saksbehandlings- og kontrollmekanismene fremstår hensiktsmessige.

Stortingets kontrollutvalg for etterretnings-, overvåkings- og sikkerhetstjeneste (EOS-utvalget) reiser spørsmål ved om inngrepet burde vært ledsaget av ytterligere vilkår for å ivareta borgernes personvern og rettsikkerhet – og i forlengelsen sikre mulighet for reell kontroll fra utvalget. Hvis tankegangen fra de nyeste EMD-dommene legges til grunn, bør det ved bruk til forebygging og etterforsking legges inn ytterligere rettssikkerhetsgarantier. EOS-utvalget påpeker at de ikke er en garantist for at feil ikke skjer eller ikke kan skje i EOS-tjenestene, og at utvalgets eksterne kontroll ikke erstatter den forvaltningsmessige styringen og kontrollen av PST.

Norges institusjon for menneskerettigheter (NIM) bemerker at forslaget ikke inneholder noen begrensninger på hvordan søk skal foregå eller gjennomføres. Høringsnotatet burde inneholdt avgrensninger av hvilke søkekriterier som kan benyttes, og mekanismer for å sikre at disse står i saklig sammenheng med formålet opplysningene skal uthentes for. Det er generelt et sentralt poeng at rettssikkerhetsmekanismene må fungere i praksis, herunder at garantiene mot misbruk bygges inn i systemet, og at det foreligger reelle avgrensninger av hvilke søkekriterier som kan benyttes. Slik forslaget er lagt opp, mener NIM at det gir PST en ubestemt skjønnsmyndighet uten kriterier for overprøving. Dette gjør også den foreslåtte kontrollen av søk lite effektiv som kontroll-

mekanisme, ettersom skillet mellom lovlig og ikke lovlige søk, ikke er tydelig.

Samlet mener NIM at departementets begrunnelse for å ikke innføre forhåndskontroll når det skal gjennomføres søk i det innsamlede materialet, ikke er tilfredsstillende. At informasjonen er åpen er ikke tilstrekkelig begrunnelse for å unnta forslaget fra rettssikkerhetsmekanismene som normalt kreves for etterretningsinnsamling. Forhåndskontroll med søk kan eventuelt gjøres ved at det innføres en godkjenningsordning for hvilke opplysninger, søkeord eller andre parametere som kan ligge til grunn for søk i materialet. Etter NIMs syn er det mange likhetstrekk med bulkinnsamling som indikerer at det bør iverksettes ytterligere rettsikkerhetsmekanismer.

Datatilsynet mener at etterkontroll ved EOS-utvalget samlet sett ikke er et robust nok system for å verne mot misbruk. Både fordi den er etterfølgende og at formålene er så vide at det er vanskelig å se hvilken del av PSTs kjernevirksomhet som ikke vil kunne benytte seg av opplysningene, noe som vanskeliggjør kontroll.

Forslaget innebærer også unntak fra rettsikkerhetsgarantier som underretning og innsyn. Datatilsynet mener det ikke er riktig at merverdien av innsyn er begrenset fordi den enkelte selv kan søke opp informasjonen, ettersom PST vil være de eneste som sitter med en oversikt som går 15 år tilbake i tid. Internett er dynamisk og opplysningene som finnes der vil forandre seg over tid.

Datatilsynet vurderer at dette tilsammen ikke er i tråd med EMDs praksis som krever en ende til ende kontroll, hvor blant annet en uavhengig forhåndskontroll også for innhentingen og søkene vil være en sentral rettsikkerhetsmekanisme. Det mangler også en målrettethet og begrensning av innsamlingen.

Medietilsynet støtter departementets konklusjon om at det må etableres gode sikkerhetsmekanismer for å forebygge maktmisbruk, og at det må sikres at EOS-utvalget kan føre tilstrekkelig kontroll med bruken. Slik forslaget er formulert er det etter Medietilsynets vurdering behov for en klarere avgrensning og tydelig definerte kontrollmekanismer. Overvåking, slik forslaget legger opp til, er svært inngripende opp mot grunnleggende menneskerettigheter. Klare retningslinjer for hvordan og hva slags informasjon som hentes inn, hvor lenge informasjonen lagres, hvordan en KI-løsning sammenstiller dataene og hvordan dataene sikres, er sentrale spørsmål, både i mandatet til PST, men også i et kontrollperspektiv. Medietilsynet støtter EOS-utvalgets innspill om at utvalgets arbeidsmåte og ressurser ikke står i forhold til omfanget av PSTs overvåking, og at kontrollfunksjonen i større grad må utredes.

Advokatforeningen er ikke enig i departementets konklusjon om at forslaget ikke innebærer aspekter som gjør EMDs uttalelser om at inngrepet i individets rettigheter etter EMK artikkel 8 tiltar underveis i prosessen, overførbare. Selv om EMDs uttalelser gjelder bulkinnsamling av grensekryssende informasjon relatert til en annen form for masseinnhenting, vil innsamlingen og potensiell bruk av opplysningene åpenbart medføre at inngrepet i individets rettigheter tiltar etter hvert som det gjøres søk i opplysningene og disse benyttes for formålene. Dersom forutgående kontroll av søk og bruk av opplysningene ikke skal innføres som kontrollmekanisme, er Advokatforeningen av den oppfatning at det blir særskilt viktig at all bruk av opplysninger registreres og kan spores, samt at registreringer faktisk gjennomgås regelmessig med det formål å avdekke eventuell uautorisert tilgang til og bruk av opplysningene som foreslått.

Advokatforeningen mener at det bør sikres at EOS-utvalgets budsjettrammer legger til rette for at en slik regelmessig kontroll utføres i praksis for å sikre at tilgangen og bruken av informasjonen skjer i henhold til de formålene og i tråd med de kravene som er satt.

Advokatforeningen foreslår at departementet vurderer å lovfeste krav til at de foreslåtte hjemlene og bruken av disse skal evalueres etter en nærmere angitt tidsperiode, eksempelvis 5 år. Et slikt evalueringskrav skal omfatte vurdering av om hovedformålet med hjemlene oppfylles, og om de etablerte kontrollmekanismene fungerer tilfredsstillende. *Rettspolitisk forening* stiller seg bak Advokatforeningens høringssvar.

Dataforeningen mener at det ikke er foreslått tilstrekkelige tiltak til å redusere risikoen ved den foreslåtte innsamlingen. I tillegg er Dataforeningen bekymret for den løpende kontrollen med et slikt regime – EOS-utvalget bevilges ikke nok ressurser, og kan kun uttale seg med anbefalinger basert på stikkprøver. Dataforeningen mener forslaget må styrkes vesentlig med hensyn til mekanismer for saksbehandling og garantier for rettssikkerhet knyttet til den foreslåtte innsamling og bruk av åpent tilgjengelig informasjon. Dataforeningen mener at det bør etableres klare kriteria for en uavhengig forhåndskontroll av adgangen til å gjøre søk mot enkeltpersoner og bruk av innsamlede opplysninger i etterforsking av konkrete saker som faller inn under PST sitt ansvarsområde.

IKT-Norge mener at mangelen på kontrollmekanismer kan være negativt for norsk næringsliv. Det legges ikke opp til noen særskilt kontroll med innsamlingen eller PSTs bruk av det innsamlede materialet, utover EOS-utvalgets kontroll. Særlig i lys av at det også foreslås unntak fra kravene til kvalitet og kravene tilknyttet behandling av særlige kategorier av personopplysninger, fremstår dette som noe underlig. Det kan med fordel utredes om den enkelte sak hvor PST ønsker tilgang til materialet, bør underlegges domstolskontroll.

Tekna merker seg at EOS-utvalget i sin høringsuttalelse finner det nødvendig å avgrense sitt ansvar ved å påpeke at deres kontroll er stikkprøvebasert og at de ikke er en garantist for at feil ikke kan skje. Tekna mener dette ikke er tilstrekkelig, og at det er viktig at utvalget får kapasitet og ressurser til å utføre tilsynsrollen på en god måte. Det bør også vurderes å gjøre tilsynsanalysene som utføres åpent tilgjengelig for allmenheten.

Tekna mener at mekanismene som er foreslått for kontroll og etterprøving ikke er tilstrekkelige. Det bør tydeliggjøres hvordan man skal sikre at kontrollmekanismene er på plass før datainnsamling starter, og avklares hvordan man kan sikre en bedre kontroll enn EOS-utvalget selv mener de har anledning til å gjennomføre. Videre er det viktig å sikre åpenhet om bruk av leverandører og innretning av algoritmer.

8.7.3 Departementets vurderinger

Departementet understreker viktigheten av gode kontrollmekanismer, rutiner og retningslinjer internt i PST, både når det gjelder innhentingen, bruken av opplysningene og sletting. PSTs internkontroll er styrket de senere år, blant annet ved at det er opprettet en ny enhet som skal ha ansvar for internkontroll og risikostyring i tjenesten. I tillegg fører Justis- og beredskapsdepartementet overordnet kontroll med tjenesten gjennom den alminnelige etatsstyringen av PST.

Som EOS-utvalget har påpekt, er utvalget ikke noen garantist for at ikke feil kan skje, eller en erstatning for god internkontroll. PST må derfor etablere rutiner som sikrer at det er notoritet over all bruk av opplysninger fra systemet med de sperrede opplysningene, slik at det på en enkel måte kan foretas kontroll av bruken. Videre forutsetter departementet at PST har løpende dialog med EOS-utvalget slik at det sikres at systemene innrettes på en måte som gjør at utvalget kan ivareta sine kontrolloppgaver.

Som omtalt i høringsnotatet oppstiller både politiregisterloven og politiregisterforskriften en rekke krav til informasjonssikkerhet og internkontroll som også vil gjelde for behandling av de sperrede opplysningene. Denne typen krav er det derfor ikke nødvendig å regulere særskilt for behandling etter den nye bestemmelsen. I tillegg er PST underlagt særskilte krav til informasjonssikkerhet i sikkerhetsloven som følge av de behandler sikkerhetsgradert informasjon i sine systemer. Det følger av politiregisterforskriften § 40-13 at all bruk av opplysninger skal registreres og kunne spores for å kontrollere om søkene er tillatt eller ikke. Videre skal registreringene gjennomgås regelmessig med det formål å avdekke uautorisert tilgang til opplysningene. Dette vil bli regulert i forskrift slik at det tydelig fremgår at denne bestemmelsen også gjelder for PST i denne sammenheng.

Det er flere av høringsinstansene som etterlyser en vurdering av om det bør etableres en ordning med uavhengig forhåndskontroll både av innhentingen og bruken av opplysningene. Som omtalt i punkt 8.3.3 og 8.6.3 anser departementet at det ikke er behov for å innføre krav om uavhengig forhåndskontroll med innhenting eller bruk av opplysningene. Det legges til grunn at det vil være tilstrekkelig med gode interne rutiner og dokumentasjon for det som hentes inn. Hva som til enhver tid ligger i det atskilte systemet vil også kunne kontrolleres, og departementet mener dette, sammen med logging av bruk og tilgangskontroll, er en mer egnet sikkerhetsmekanisme i denne sammenheng.

EOS-utvalget har påpekt at det er viktig at adekvat sperrefunksjonalitet er på plass i PSTs systemer før innhentingen settes i gang, og at utvalget må kunne kontrollere sperrefunksjonaliteten. Departementet er enig i dette. Det må sikres at opplysningene holdes helt atskilt fra PSTs øvrige systemer, altså at det etableres en egen «boks» for disse opplysningene, før innhentingen starter. Det er videre sentralt at PST tilrettelegger systemene for EOS-utvalgets kontroll.

Når det gjelder bruken av opplysningene, må det etableres rutiner som sikrer at det kun foretas søk i systemet ut i fra konkrete informasjonsbehov av personer som er bemyndiget til å foreta søkene. I tillegg til bemyndigelse vil personene som har tilgang være underlagt taushetsplikt og være sikkerhetsklarert for høyeste nivå. For å sikre kontroll med hvem som har foretatt søk og hvorfor søket er foretatt, må dette kunne dokumenteres og foreligge i en form som til enhver tid kan kontrolleres. Dersom det foretas søk, eksempelvis på bakgrunn av et konkret tips, som resulterer i at det opprettes en forebyggende sak eller

etterforskingssak må saken besluttes opprettet i tråd med gjeldende regler, og opplysningene må flyttes over i PSTs vanlige registre og følge reglene for behandling der. Det må sikres notoritet over hvilke saker som er opprettet og hvilke opplysninger som er flyttet over i ordinært register, slik at dette kan kontrolleres internt i PST og av EOS-utvalget på vanlig måte. All bruk av opplysningene vil dessuten måtte logges og kunne spores.

I EMDs praksis vedrørende bulkinnsamling er det lagt til grunn at etterfølgende kontroll må gjennomføres av et uavhengig organ. Det oppstilles ikke som vilkår at kontrollen må skje av en uavhengig domstol. Det sentrale i de to kriteriene om etterfølgende kontroll er at kontrollen må gjennomføres av et uavhengig organ, og at kontrollorganet har reelle og formelle fullmakter til å vurdere etterlevelsen av de formelle kravene i lovgivningen, samt vurdere forholdsmessigheten av eventuelle inngrep. Videre oppstilles det krav om reell etterkontroll av behandlingen av opplysningene og klagerett for den enkelte.

EOS-utvalget er et uavhengig organ opprettet av Stortinget, og kan kontrollere alle deler av PSTs virksomhet. Selv om EOS-utvalget ikke kan treffe bindende avgjørelser overfor forvaltningen, er det utviklet gode og effektive systemer for å følge opp rapporterte avvik. I tillegg avgir utvalget årlig en melding til Stortinget om sin virksomhet, herunder om kontroll med PST. Utvalget kan også gi særskilte meldinger dersom det er avdekket forhold hos PST som Stortinget straks bør kjenne til. Den etterfølgende kontrollen ved PSTs virksomhet foretas gjennom inspeksjoner, klagesaker og behandling av saker som tas opp av eget tiltak. Enkeltpersoner kan be utvalget kontrollere om opplysningene om vedkommende er behandlet i samsvar med loven. Det er også anledning til å reise sak for domstolene. Samlet sett mener derfor departementet at de eksisterende mekanismene for uavhengig kontroll ivaretar de krav som følger av EMDs praksis.

Hva gjelder den enkeltes mulighet til å begjære kontroll med opplysningene, følger det av politiregisterloven § 68 at EOS-utvalget, etter begjæring fra *den registrerte eller den som antar å være registrert*, skal kontrollere om opplysningene om vedkommende er behandlet i samsvar med loven. En sentral følge av at opplysningene er sperret er at personer ikke skal anses registrert hos PST, og at det for personer som kun finnes i det sperrede materialet, derfor i utgangspunktet heller ikke er noe å kontrollere. Departementet har vurdert om det bør etableres særskilte regler for at EOS-utvalget kan føre kontroll med om opplysninger om konkrete enkeltpersoner finnes i det sperrede materialet. Imidlertid ville en slik kontrollmekanisme ha liten reell effekt. Ettersom det åpnes for innsamling av store mengder informasjon, der det ikke er konkrete vilkår knyttet til innsamling og lagring ut over at behandlingen må antas å være nødvendig for analyser og etterretningsvurderinger, vil kontrollen kun gå ut på å undersøke om det ligger opplysninger om vedkommende i opplysningene som er sperret. I og med at opplysningene ikke er underlagt krav til individuell vurdering, vil resultatet være at kontrollen ikke gir grunnlag for kritikk, uavhengig av om det ligger opplysninger i materialet eller ikke. Videre vil det være vanskelig for PST å verifisere om den enkelte opplysning faktisk knytter seg til den personen som ber om kontrollen. Opplysningene vil ikke ligge strukturert, og det vil i mange tilfeller ikke være mulig å fastslå hvilken person en opplysning knytter seg til. For å sikre en entydig identifikasjon kan det bli behov for å samle inn enda flere opplysninger om vedkommende, noe som kan medføre ytterligere inngrep overfor den som ber om kontrollen.

EOS-utvalget har imidlertid, i tråd med EOS-kontrolloven, innsyn i og kan kontrollere ethvert system, register, arkiv, installasjoner mv., samt PSTs behandling av personopplysninger. Utvalget kan dermed kontrollere opplysninger om enkeltpersoner i det atskilte systemet. Ettersom innhentingsadgangen er såpass vid vil det likevel være vanskelig å vurdere den enkelte opplysning som ligger i det sperrede materialet, og departementet mener at det vil ha mer for seg å kontrollere hva opplysningene faktisk er brukt til etter at de er hentet ut av systemet. Opplysninger som er flyttet over i PSTs alminnelige systemer vil EOS-utvalget kunne kontrollere på vanlig måte.

Hva gjelder algoritmer og leverandører av systemer vil også dette kunne kontrolleres av EOS-utvalget. Det følger av EOS-kontrolloven § 6 annet ledd at utvalgets kontroll skal omfatte tjenestens tekniske virksomhet, herunder overvåking og innhenting av informasjon og behandling av personopplysninger.

Departementet opprettholder at det ikke er grunn til å gjøre unntak fra dagens hovedregel om at det ikke er innsyn i opplysninger som behandles hos PST. Når innhentingen er mer begrenset og informasjonen lagres i kortere tid, gjør argumentene mot innsyn seg enda sterkere gjeldende. Innsyn vil kunne innebære en risiko for at det avsløres hvilke områder på nettet PST velger å laste ned informasjon fra, slik at trusselaktører til-

passer sin aktivitet ut fra dette. Videre vil det som nevnt være vanskelig og ressurskrevende å identifisere om opplysningene faktisk gjelder den personen som ber om innsyn, samtidig som merverdien for den enkelte vil være begrenset.

8.8 Sletting

8.8.1 Forslaget i høringsnotatet

I høringsnotatet ble det vist til at det vil være behov for å lagre opplysninger over tid for å kunne følge med på utvikling og endringer i trusselbildet. Enkelte typer trusler og aktivitet som det er ønskelig at PST skal kunne kartlegge, som påvirkningsoperasjoner fra andre land og ulovlig etterretningsvirksomhet, kan pågå over flere år. Dersom en ny type trussel oppstår, kan informasjon tilbake i tid være av stor betydning for å kunne vurdere og forutse fremtidig utvikling innenfor feltet. Det er derfor vanskelig å sette en klar grense for hvor lenge opplysningene vil anses nødvendige for etterretningsformål, og departementet mente at det er viktig at opplysningene ikke slettes så tidlig at formålet med forslaget ikke oppnås. Samtidig ville for lang lagringstid kunne innebære at inngrepet etter hvert anses uforholdsmessig.

Det ble foreslått at opplysningene skal slettes senest etter 15 år, tilsvarende reglene i etterretningstjenesteloven § 9-8 om sletting av rådata i bulk. Det ble understreket at 15 år er en lengstefrist. Etterretningstjenesteloven § 9-8 åpner for å lagre informasjonen ut over 15 år dersom vesentlige hensyn tilsier at sletting utsettes. Departementets foreløpige vurdering i høringsnotatet var at det ikke var behov for å åpne for en mulighet for forlenget lagring av opplysninger som behandles etter den nye bestemmelsen.

8.8.2 Høringsinstansenes syn

Forsvarsdepartementet, Datatilsynet, Stortingets kontrollutvalg for etterretnings-, overvåkings- og sikkerhetstjeneste (EOS-utvalget), Kripos, Medietilsynet, Nasjonal kommunikasjonsmyndighet (NKOM), Norges institusjon for menneskerettigheter (NIM), Politidirektoratet, Advokatforeningen, Den Norske Dataforening, Elektronisk Forpost Norge, Rettspolitisk forening, Tekna og *UTSYN* har uttalt seg om slettefristen. Nær samtlige av høringsinstansene mener at fristen er for lang.

Forsvarsdepartementet har ikke synspunkter på når slettefristen bør inntre, men mener det er nærliggende å påpeke at E-tjenesten behandler opplysninger for et annet formål enn PST, og at etterretningstjenesteloven § 5-3 har klare vilkår for behandling av data i bulk. Tilsvarende behandlingsregler synes å mangle i lovforslaget her. Det bør vurderes om man eventuelt kombinert med en kortere slettefrist bør innta en bestemmelse om fristforlengelse knyttet til nærmere vilkår. Også *Medietilsynet* mener en kortere lagringstid bør vurderes, og at man eventuelt kan vurdere å innta unntaksbestemmelser for opplysninger som det av særlige grunner er viktig at kan lagres lenger.

Politidirektoratet kan ikke se at behovet for en så vidt lang lagringstid er tilstrekkelig begrunnet, og at det i vurderingen av lagringstid bør legges vekt på at graden av inngrepet blir større jo lenger opplysningene lagres. Politidirektoratet og *Kripos* anbefaler at departementet ytterligere begrunner behovet for en så lang lagringstid.

Datatilsynet kan ikke se noen tungtveiende begrunnelse for en så lang lagringstid som 15 år. Når det gjelder henvisningen til etterretningstjenesteloven § 9-8 om sletting av rådata i bulk, så omfatter «rådata i bulk» lite informasjon om norske borgere, noe som heller ikke er formålet med innsamlingen. Hvis en skal velge en bestemmelse fra etterretningsloven som inspirasjon er § 7-7 om innhenting og lagring av metadata i bulk etter tilrettelagt innhenting mer relevant, med en lagringstid på 18 måneder. Også *Dataforeningen* mener lagringstiden bør være vesentlig kortere, og viser til etterretningstjenesteloven § 7-7.

EOS-utvalget savner en faglig begrunnelse for lengden på fristen. I vurderingen av hvor lenge opplysningene kan beholdes, mener utvalget det er relevant å legge vekt på at inngrepet overfor den enkelte borger blir større jo lenger opplysningene lagres. Utvalget vil påpeke at ved innføring av en ny metode med en lengstefrist for sletting, er det viktig at fungerende slettefunksjonalitet er på plass i PSTs systemer før innhenting settes i gang. EOS-utvalget må også kunne kontrollere slettefunksjonaliteten.

NIM mener lagringstiden er for lang, og viser til at inngrepet vil være større jo lengre lagringstid det åpnes for, samtidig som det reelle behovet for opplysningene gjerne vil være redusert. Risikoen for formålsutglidning i hva opplysningene kan brukes til vil også øke jo lenger lagringstid det er tale om. Også øvrige rettssikkerhetshensyn, slik som muligheten for å verifisere opplysningenes sannhet, kan gjøre lang lagringstid mer betenkelig. Det er ikke gitt noen nærmere redegjørelse for behovet for en såpass lang frist som 15 år. Så lenge forslaget ikke inneholder noen

plikt til å revidere og slette materialet innenfor denne fristen må det legges til grunn at store deler av innsamlede opplysninger vil beholdes ut lengstefristen.

Advokatforeningen, *Rettspolitisk forening* og *UTSYN* mener lagringsperioden på 15 år er for lang og i liten grad begrunnet. *Advokatforeningen* peker på at jo lenger tid som går, jo vanskeligere vil det også være å kontrollere om opplysningene er korrekte. For en registrert person vil det også være svært vanskelig å forholde seg til, og eventuelt forsvare seg mot, informasjon som er gammel.

Advokatforeningen og *Rettspolitisk forening* mener at det er uklart hvordan sletteregelen skal anvendes dersom PST genererer ny informasjon av gammel informasjon, eksempelvis ved berikelse av data, eller der gammel informasjon sammenstilles med annen informasjon av nyere dato.

Tekna viser til at ved langvarig lagring vil dataene kunne anses tatt ut av tidligere kontekst, være lite representative, og kan for eksempel være dårlig formulerte kommentarer på en nettside som man selv har slettet eller redigert etter kort tid. Tidshorisonten fremstår uforholdsmessig lang, og kan oppfattes som en form for langvarig overvåking.

Tekna stiller også spørsmål ved hvilket tidspunkt man legger til grunn for tidsberegningen og hvordan dette skal implementeres i praksis. Tekna mener videre at mellomlagret informasjon må slettes når bruken i et etterretningsoppdrag, forebyggende sak eller etterforskning er ferdig. Dette er spesielt viktig ved etterretningsoppdrag, ettersom disse inneholder informasjon om langt flere personer. *Elektronisk Forpost Norge* har lignende synspunkter.

NKOM mener det er uklart når fristen begynner å løpe i forbindelse med oppretting av sak, og om det er ment at lagring i 15 år vil være den ytre ramme.

8.8.3 Departementets vurderinger

For at PST skal kunne identifisere eventuelle avvik fra normalsituasjonen, må PST ha et godt bilde av denne. Dette vil være enklere jo lenger tilbake i tid man har mulighet til å se data. Lagringstiden vil også ha betydning ved bruk av automatiserte analyseverktøy. Jo flere data som er tilgjengelig, og jo lenger tidsrom dataene stammer fra, jo mer erfaring har man å bygge på når man skal utvikle en modell for å forstå et fenomen. Bruk av informasjon for å kunne vise trender og utvikling i trusselvurderingssammenheng er avhengig av at dataene lagres i noe tid. Jo lenger tilbake i tid man har data, jo lenger frem i tid vil man kunne predikere utviklingen. Departementet mener derfor at det er viktig at lagringstiden ikke blir for kort til at PST kan nyttiggjøre seg informasjonen. 18 måneders lagringstid, slik som etter etterretningstjenesteloven § 7-7, vil ikke være tilstrekkelig til å imøtekomme behovet. Departementet mener at det heller ikke er egnet med en mellomlagring til et konkret «oppdrag», og at opplysningene deretter slettes. En slik begrenset behandling kan tenkes å være aktuelt i enkelttilfeller, men vil ikke være egnet i alle sammenhenger.

Samtidig må lagringstiden avveies mot det inngrepet forslaget utgjør. Som en rekke instanser har pekt på vil inngrepet for den enkelte bli større jo lengre dataene lagres. Jo lenger opplysningene er lagret, jo større er sannsynligheten for at informasjonen er utdatert eller slettet på det åpne nettet. Departementet har derfor vurdert lagringstiden på nytt, og kommet til at opplysningene bør slettes senest etter fem år. Dette tilsvarer fristen som gjelder for når opplysninger utenfor forebyggende sak, der det ikke er registrert nye opplysninger om personen, må gjennomgås, jf. politiregisterforskriften § 22-3 tredje ledd. Også fem år er lang tid. Samtidig er det i andre sammenhenger akseptert at PST, på grunn av sin særlige virksomhet, må kunne behandle opplysninger over lengre tid. Det vises til Ot.prp. nr. 108 (2008–2009) punkt 17.3.1.1 på side 272, der det i forbindelse med nødvendighetskravet ved behandling av opplysninger i forebyggende sak er uttalt:

> «[…] nødvendighetsvurderingen for PST må skje i et vesentlig lenger tidsperspektiv enn for politiet for øvrig. Årsaken er at de som står bak sikkerhetstruslene arbeider langsiktig, og for tidlig sletting av usikker informasjon som senere kunne vist seg å ha hatt en vesentlig kriminalitetsbekjempende verdi, vil være svært uheldig på et område som gjelder grunnleggende sikkerhetsinteresser. I tidsperspektivet ligger også at de som står bak truslene, særlig på etterretningssiden, også driver en lovlig virksomhet, dels i tillegg til og dels som dekke for, den ulovlige virksomheten. For å være i stand til å vurdere hva som konkret har sammenheng med ulovlig virksomhet, er det nødvendig å vurdere virksomheten i en helhet, og følgelig vil det over noe tid også være behov for å kartlegge og behandle opplysninger om lovlig virksomhet hos dem som mistenkes for å forberede og utføre ulovligheter.»

Slettefristen er en lengstefrist, slik at opplysningene vil måtte slettes tidligere dersom det er klart at de ikke har betydning for utarbeidelse av analyser og etterretningsvurderinger. Dette innebærer ikke at PST fortløpende må vurdere om opplysningene skal slettes, men plikt til å slette før fristen kan for eksempel inntre dersom PST laster ned et kryptert datasett som ut fra tittel, forfatter eller lignende antas å ha betydning, men der PST etter å ha åpnet filene ser at datasettet ikke inneholder noen opplysninger av verdi. Det samme gjelder dersom det ikke er noe behov for å beholde et datasett etter at en analyse eller etterretningsvurdering på et område er ferdigstilt.

I høringsnotatet ble det vist til at departementets foreløpige vurdering var at det ikke var behov for en mulighet til å beslutte utsatt sletting, slik det finnes i etterretningstjenesteloven § 9-8. Når slettefristen nå blir atskillig kortere, finner departementet at det bør være en åpning for å beslutte utsatt sletting, slik også Forsvarsdepartementet og Medietilsynet har påpekt. Det er på det rene at en slettefrist på fem år i noen tilfeller vil kunne være for kort, for eksempel vil det kunne være vanskelig å kartlegge påvirkningsvirksomhet i tilknytning til valg over flere valgperioder. For slike behov bør det være mulig å beslutte at nærmere bestemte opplysninger skal beholdes i en lengre periode.

En beslutning om utsatt sletting forutsetter at opplysningene etter en konkret vurdering fortsatt er nødvendige for utarbeidelse av analyser og etterretningsvurderinger. Utsatt sletting vil derfor representere et unntak. Samtidig må det etter departementets syn settes en ytre ramme for hvor lenge de sperrede opplysningene kan være lagret. Det foreslås derfor at de sperrede opplysningene ikke kan beholdes lenger enn 15 år totalt. Det er viktig at det er notoritet om beslutninger om utsatt sletting, og departementet tar derfor sikte på å regulere i forskriften at slike beslutninger skal være skriftlig og begrunnet.

Departementet understreker at slettefristen etter den nye bestemmelsen gjelder opplysningene som er sperret. Slettefunksjonalitet vil måtte bygges inn i systemet og kunne kontrolleres, slik EOS-utvalget påpeker. Dersom opplysningene tas i bruk i forebyggende sak eller i etterforsking, jf. forslaget til § 65 a annet ledd nr. 2 og 3, vil de måtte flyttes over i og behandles i PSTs ordinære systemer, og de alminnelige slettereglene vil gjelde for disse opplysningene. Når det gjelder de ferdige analysene og vurderingene som er laget på bakgrunn av opplysningene, vil den generelle regelen om at opplysningene skal slettes når de ikke lenger er nødvendige for formålet komme til anvendelse. Departementet vil vurdere å tydeliggjøre disse forholdene i forskriften. Departementet tar også sikte på å tydeliggjøre at sletting av opplysninger som er sperret etter den nye bestemmelsen skal skje i form av tilintetgjøring, slik at disse ikke skal avleveres til Arkivverket og bevares for ettertiden, jf. politiregisterforskriften § 16-2 annet ledd nr. 2.

8.9 Bruk av automatiserte analyseverktøy

8.9.1 Forslaget i høringsnotatet

I høringsnotatet ble det vist til det vil kunne være nødvendig at behandling av opplysningene for etterretningsformål skjer helt eller delvis ved hjelp av automatiserte metoder. Forslaget la ikke føringer på hvordan opplysningene skal behandles for å ivareta etterretningsformålet. Av pedagogiske hensyn ble det likevel foreslått å innta i politiregisterforskriften at behandling for etterretningsformål kan skje ved bruk av automatiserte analyseverktøy. Det ble understreket at bruk av automatiserte analyseverktøy ikke kan skje med det formål å kartlegge enkeltindividers aktivitet på nett.

8.9.2 Høringsinstansenes syn

Forsvarsdepartementet savner en nærmere vurdering av om automatisk behandling av åpent tilgjengelig informasjon bør kunne benyttes for etterforskings- og forebyggingsformål. Forsvarsdepartementet skulle også gjerne sett en mer utfyllende beskrivelse av hva som menes med automatiserte analyseverktøy, og om dette kan inkludere for eksempel bildegjenkjenning og ansiktsgjenkjenning, herunder bruk av kunstig intelligens.

Digitaliseringsdirektoratet (Digdir) viser til at regelverk som en klar hovedregel bør utformes teknologinøytralt. Digdir er derfor kritiske til regulering av bruk av automatiserte analyseverktøy av pedagogiske hensyn, da det kan bidra til at det stilles spørsmål ved om bruk av metoder som ikke er nevnt er tillatt. Om bestemmelsen beholdes, kan det med fordel gå klarere fram hvilken type automatisert behandling bestemmelsen tillater.

Stortingets kontrollutvalg for etterretnings-, overvåkings- og sikkerhetstjeneste (EOS-utvalget) mener at bruk av automatiserte analyseverktøy reiser rettslige, tekniske og kontrollrelaterte problemstillinger. Utvalget peker på at det er nødven-

dig at PST tilrettelegger sine systemer for kontroll ved å bygge inn kontrollmuligheter som del av systemene, og at dette også gjelder eventuelle automatiserte analyseverktøy.

Datatilsynet påpeker at verktøyene i liten grad er beskrevet. Det er derfor vanskelig å si hvor grensen for de ulike søkene og analyseverktøyene går. Det fremstår som uklart om PSTs behandling innebærer profilering. Høringsnotatet behandler ikke hvordan den forslåtte behandlingen skal reguleres slik at den blir i samsvar med politidirektivet og de generelle prinsippene knyttet til profilering i personvernforordningen. Et perspektiv som ikke i tilstrekkelig grad er drøftet, er hvordan en automatisert innsamling og analyse av ytringer og handlinger som for eksempel å være medlem av en gruppe vil kunne gi opplysninger som den enkelte ikke ønsker å dele med offentligheten.

Norges institusjon for menneskerettigheter (NIM) legger til grunn at automatiserte analyseverktøy vil kunne omfatte verktøy basert på maskinlæring/kunstig intelligens. En iboende risiko ved automatiserte analyseverktøy er diskriminering og forutinntatthet. I EU-kommisjonens etiske retningslinjer for kunstig intelligens, som også ligger til grunn for Nasjonal strategi for kunstig intelligens, anbefales blant annet at kunstig intelligens som bygger på personopplysninger, eller som retter seg mot personer, skal følge personvernforordningen. Videre anbefales det at identifiserbare og diskriminerende skjevheter bør fjernes i innsamlingsfasen av datasett. Bruk av slike verktøy for kriminalitetsbekjempelsesspørsmål reiser særlige spørsmål. Etter NIMs oppfatning bør automatiske analyseverktøy bygge på etiske prinsipper, og utformes med tanke på menneskerettighetene. NIM savner i lys av disse grunnleggende utfordringene en nærmere beskrivelse av analyseverktøyene, hvordan disse tenkes brukt, herunder hvilke mekanismer som er tenkt iverksatt for å forhindre og redusere diskriminering, misvisende resultater eller andre uønskede utfall ved bruk av slike verktøy, herunder falsk og villedende informasjon.

Advokatforeningen mener at det bør lovfestes begrensninger for bruken av visse typer teknologi, eksempelvis teknologi med kunstig intelligens som i praksis er egnet for masseovervåking. I den forbindelse fremheves det at EU-kommisjonens forslag til forordning om bruk av kunstig intelligens, vil få betydning også innenfor offentlige samfunnsområder. Bruk av kunstig intelligens innenfor politi og annen myndighetsutøvelse vil være definert som høyrisiko på noen områder, og forslaget fra EU-kommisjonen forutsetter da etablering av risikohåndtering og en rekke andre krav. Advokatforeningen mener på denne bakgrunn at departementets forslag må gi klarere føringer på hvilke typer teknologi det skal være tillatt å benytte, samt relevante tilleggskrav ved bruk av teknologi som innebærer høy risiko.

Dataforeningen mener at forslaget i begrenset grad beskriver de verktøyene som skal benyttes, og den teknologiske utviklingen og utviklingen i bruk av maskinlæring og kunstig intelligens vil medføre stadig mer inngripende muligheter. Bruk av analyseverktøyene vil skape ny informasjon om enkeltpersonene, uten at de selv er informert om dette. De etiske prinsippene som bør legges til grunn for bruk av kunstig intelligens til analyse av de innsamlede dataene burde vært drøftet, og forslagene burde inneholdt krav til eventuell bruk av kunstig intelligens for analyseformål og til etterfølgende bruk for etterforskingsformål.

Dataforeningen mener at loven bør fastsette hvorledes den foreslåtte behandlingen skal reguleres, slik at den blir i samsvar med politidirektivets artikkel 11 og de generelle prinsippene knyttet til profilering i personvernforordningen. Dataforeningen mener at det eksplisitt må avgrenses mot at automatiserte metoder skal kunne benyttes til å identifisere personer som det skal opprettes forebyggende sak mot. Mangelen på transparens, risikoen for feil og risiko for at fordommer i algoritmene har en diskriminerende effekt medfører et betydelig tilbakeskritt for rettssikkerheten.

IKT-Norge mener at det at forslaget åpner for at PST kan bruke algoritmer på store mengder data om samtlige borgere for å finne sannsynligheter for mulige kriminelle handlinger i fremtiden, aktualiserer andre problemstillinger enn om man bruker teknologien til å målrettet søke tilbake i tid for etterforskning av spesielle miljøer eller konkrete personer. Automatisk profilering og beslutninger gir risiko for uberettiget mistanke og diskriminering. IKT-Norge vil fremheve risikoen for nedkjølingseffekt, og redusert tillit i samfunnet, dersom det ikke oppstilles sterke rettssikkerhetsgarantier for å forhindre uberettiget mistanke og diskriminering som følge av bruk av slike verktøy.

IKT-Norge mener at lovforslaget er tvetydig når det gjelder hva automatiske analyseverktøy skal og ikke skal kunne brukes til. Dersom høringsnotatets definisjon av etterretningsformål legges til grunn, vil PST avskjæres fra å bruke automatiserte analyseverktøy opp imot enkeltpersoner. Vernet som her tilsynelatende oppstilles, uthules imidlertid av at PST likevel kan bruke

opplysninger de «kommer over» for etterretningsformål, til å registrere enkeltpersoner i PSTs øvrige registre.

IKT-Norge mener at det er uklart i hvilken utstrekning man har ment å tillate bruken av automatiserte analyseverktøy til å etterforske og forfølge enkeltpersoner, og hvilke rettssikkerhetsgarantier som i så fall skal gjelde. Bruken av slike verktøy reiser etiske problemstillinger som i liten grad er berørt. Etter IKT-Norges mening må det gjøres tydeligere hva PST skal ha adgang til å bruke automatiserte analyseverktøy til. Dersom bruk av automatiserte analyseverktøy mot enkeltpersoner skal tillates, forutsetter det i alle tilfelle en klar hjemmel i lov.

NITO ser det som uklart hvordan en teknolog skal skrive en algoritme som følger med på trender uten at det også følges med på individer. NITO er bekymret for faren for feil, og risiko ved å stole blindt på «output» fra en kunstig intelligens. NITO viser i den anledning til EUs AI regulativ Annex III. Systemet som trengs for å analysere dataene her vil mest sannsynlig ikke er lovlig etter dette EU-regulativet. En kjerne i dette er risiko for at PST feilaktig flagger og kategoriserer personer som farlige eller presumtivt kriminelle basert på datainnsamling og -analyse, spesielt hvis denne blir gjennomført av en mer eller mindre trent kunstig intelligens.

Tekna uttaler at bruk av automatiserte analyseverktøy vil generere nye data om enkeltpersoner, som personen ikke har valgt å dele åpent. Ulike problemstillinger knyttet til bruk av automatiserte analyseverktøy er ikke utredet i forslaget. Det bør avklares i loven om det gis adgang til profilering, jf. personvernforordningen artikkel 22.

Anskaffelse av analyseverktøy kan i seg selv gi grunn til bekymring. Bruk av verktøy som er utviklet og driftes av aktører i andre land, åpner opp en rekke spørsmålsstillinger knyttet til personvernforordningen, dataeierskap med mer. Tekna mener derfor at det bør være åpenhet om valg av leverandør av analyseverktøy.

8.9.3 Departementets vurderinger

Flere av høringsinstansene har stilt spørsmål ved hva som menes med automatiserte analyseverktøy, og om forslaget innebærer at det kan benyttes profilering, bruk av kunstig intelligens mv. Noen fremholder at det bør lovfestes hvilke metoder som kan benyttes og ikke, særlig når det gjelder bruk rettet mot enkeltpersoner. Departementet vil derfor innledningsvis presisere at behandlingsbegrepet, slik dette er definert i politiregisterloven § 2 nr. 2, omfatter enhver behandling av opplysninger, herunder også automatisert behandling og analyse. I utgangspunktet er det derfor ikke behov for å regulere automatiserte metoder for at slike skal kunne benyttes.

Begrunnelsen for likevel å regulere bruk av slike verktøy, er behovet for å synliggjøre at det ikke vil være mulig å «følge med» på internett eller analysere store mengder informasjon for å følge med på trender og utvikling, ved manuelle metoder. Mengden data fordrer at dataene må systematiseres og sees i sammenheng for å kunne avdekke ukjente sammenhenger og avvik fra en «normalsituasjon». Bearbeiding av informasjonen slik at ulike opplysninger kan sees i sammenheng, vil være en forutsetning for at dataene som innhentes kan komme til nytte. Det vil i mange tilfeller ikke være mulig å se på utvikling over tid uten hjelp av automatiserte verktøy. Formålet er å kartlegge trender og utviklingstrekk for å benytte informasjonen til å utarbeide analyser og etterretningsvurderinger om forhold i Norge som kan true nasjonale sikkerhetsinteresser. Formålet med behandlingen er dermed ikke individrettet. Samtidig vil informasjonen som analysene lages på bakgrunn av, inneholde personopplysninger. Gitt mengden data som kan samles inn, vil det ikke være mulig å anonymisere opplysninger om enkeltpersoner for så å foreta ulike analyser. Analysene vil således berøre enkeltindivider, selv om formålet ikke er å danne grunnlag for beslutninger på individnivå.

Forslaget åpner for at det kan utvikles og benyttes maskinlæringsmodeller. Modellene kan eksempelvis utvikles gjennom statistikk, indikatorer og vekting av disse, og basert på eldre data kunne gi en prediksjon om fremtiden. Eksempler på slike modeller kan være trendanalyser, sentimentanalyser, det vil si analyse av positive og negative holdninger, følelser og meninger, og utvikling av grafer. Slike analyser vil så være en del av den informasjonen som ligger til grunn for etterretningsvurderingene, som igjen skal gi grunnlag for beslutningsstøtte.

Departementet har etter en fornyet vurdering kommet til at adgangen til å benytte automatiserte analyseverktøy i forbindelse med utarbeidelse av analyser og etterretningsvurderinger bør inntas i lovteksten, og ikke kun i forskrift. Selv om begrepet inntas i loven, må det imidlertid tas høyde for at betydningen av begrepet kan endres over tid, ettersom den teknologiske utviklingen går svært raskt og er vanskelig å forutsi. Begrensningen til bruk til utarbeidelse av analyser og etterretningsvurderinger er derfor sentral. Departementet

bemerker at en lovfesting av at det kan benyttes automatiserte analyseverktøy i denne sammenheng knytter seg til behovet for klarhet og inngrepets karakter. Det følger ellers av politiregisterlovens system at det er *behandlingen* av opplysninger som reguleres, og ikke hvilke verktøy som kan benyttes for behandlingen. Departementet presiserer således at man med forslaget ikke tar stilling til lovfesting av andre ulovfestede metoder som PST og politiet for øvrig benytter.

At bruken av automatiserte analyseverktøy er begrenset til utarbeidelse av analyser og etterretningsvurderinger om forhold i Norge som kan true nasjonale sikkerhetsinteresser, innebærer at slike verktøy *ikke* kan benyttes for å finne personer som det kan være aktuelt å opprette forebyggende sak på, eller i forbindelse med etterforsking. Som beskrevet i høringsnotatet skal verktøyene ikke benyttes for å følge enkeltpersoners aktivitet på internett. Det kan således ikke brukes verktøy basert på profilering for å identifisere enkeltindivider eller med det formål å predikere om enkeltpersoner i fremtiden, ut fra bestemte kriterier, vil antas å begå kriminalitet. Som beskrevet ovenfor vil maskinlæringen berøre opplysninger om personer i den forstand at de vil inngå som data i maskinlæringsmodeller, men det vil ikke bli fattet beslutninger basert på modellen på individnivå. Ettersom det ikke er anledning til å benytte profilering eller på annen måte benytte automatiserte analyseverktøy til vurderinger eller avgjørelser på individnivå, vil reglene i personvernforordningen og direktiv (EU) 2016/680 artikkel 11 om automatiserte beslutninger etter departementets mening ikke få betydning i denne sammenheng. Avgrensningen mot profilering og automatiserte individuelle avgjørelser gjør også at risikoen for at feil, diskriminering, og forutinntatthet ved bruk av automatiserte analyseverktøy som er basert på kunstig intelligens vil kunne ha negative konsekvenser for enkeltpersoner, er begrenset.

Ettersom opplysningene som ligger til grunn for analysene vil inneholde personopplysninger, kan det likevel ikke helt utelukkes at en automatisert analyse avdekker personer som det er grunn til å undersøke nærmere, selv om dette ikke er formålet med og innretningen på analysen. I slike tilfeller legger departementet til grunn at PST må kunne foreta nærmere undersøkelser på vanlig måte, slik tjenesten for eksempel gjør ved tips. Det vil imidlertid ikke kunne opprettes forebyggende sak eller åpnes etterforsking *utelukkende* basert på en automatisert analyse.

Det at bruk av automatiserte *analyseverktøy* begrenses til utarbeidelse av analyser og etterretningsvurderinger, avskjærer ikke at annen behandling skjer automatisert i større eller mindre grad. Ettersom opplysningene er lagret elektronisk, vil ethvert søk som foretas i en mengde data kunne anses å være automatisert, all den tid det skjer en prosess som utføres av en maskin, applikasjon eller lignende for å vise de relevante resultatene. Forslaget her er ikke til hinder for det.

Avslutningsvis vil departementet understreke at selv om det kan benyttes automatiserte analyseverktøy ved utarbeidelse av analyser og etterretningsvurderinger, innebærer ikke dette at resultatene ikke vil bli gjennomgått og bearbeidet manuelt eller at de alene vil kunne brukes som beslutningsstøtte. Det kan oppstå feil i resultater som kommer ut av eventuelle maskinlæringsmodeller. Selv om det ikke direkte rammer enkeltpersoner ettersom det ikke kan opprettes saker kun basert på modellene, kan feil eller skjevheter i modellene gi et uriktig bilde av situasjonen, grupper mv. Analysene vil derfor kun være én kilde til informasjon, som igjen må ses i sammenheng med annen informasjon PST besitter for å kunne gi et helhetlig og korrekt bilde. Bruk av automatiserte analyseverktøy fordrer også en kontinuerlig styring av algoritmens tolkning og forståelse av begreper, samt manuell vurdering.

Hva gjelder kontroll av PSTs behandling av opplysninger i denne sammenheng, herunder bruk av eventuelle automatiserte analyseverktøy, må det legges til rette for at EOS-utvalget kan foreta reelle kontroller av disse. EOS-utvalget vil ha fullt innsyn i de systemer og algoritmer som benyttes. Ved utvikling og kjøp av nye verktøy må det sikres at kontrollbehovene ivaretas i løsningene.

9 Økonomiske og administrative konsekvenser

Forslaget om å tydeliggjøre PSTs etterretningsoppdrag i politiloven og gi en korresponderende hjemmel for behandling av opplysninger for dette formålet vil i seg selv ikke ha økonomiske eller administrative konsekvenser av betydning. Forslaget krever begrensede tekniske tilpasninger, og vil derfor kunne tre i kraft raskt etter vedtakelse. Det vil imidlertid være krevende for tjenesten å gi god beslutningsstøtte innenfor et bredere felt enn det som følger av dagens mandat, i tillegg til å forebygge og etterforske straffbare forhold etter dagens bestemmelser. Gitt dagens trusselbilde, og avhengig av hvilken ambisjon som besluttes for PSTs arbeid, vil det derfor kunne være økt behov for personell for å ivareta oppgaven fullt ut.

Forslaget om å etablere en hjemmel for behandling av åpent tilgjengelig informasjon for utarbeidelse av analyser og etterretningsvurderinger vil kreve tekniske endringer før bestemmelsene kan settes i kraft. Kostnadene vil blant annet avhenge av hvor mye informasjon som skal lagres og antall kilder. Det må etableres en ny plattform hvor de sperrede opplysningene skal ligge, som gjør det mulig å behandle opplysningene atskilt fra opplysninger som ellers behandles hos PST. Kostnadene vil fordeles på personell og teknologi, og knytter seg hovedsakelig til innhenting og behandling av opplysninger, lagring av data, analyseverktøy, analyser, maskinvare og programvare. Det vil være behov for rekruttering knyttet til utvikler- og analysekompetanse og IT-driftsressurser, i tillegg til kompetanse PST allerede besitter. Det anslås et merbehov på 15 årsverk, som tilsvarer merutgifter på om lag 23 mill. kroner årlig. Kostnadene for teknologi knytter seg til anskaffelse av hyllevare og selvutviklet program- og maskinvare, hvor det er lagringsbehovet som hovedsakelig styrer kostnaden. Investeringskostnadene til etablering av plattformen anslås til om lag 40 mill. kroner, med en påfølgende varig kostnad anslått til om lag 25 mill. kroner årlig for maskinvare og lisensiering. I tillegg til tekniske og personellmessige behov, må PST utarbeide gode rutiner og retningslinjer internt for hvordan opplysningene skal behandles.

I denne proposisjonen bes det om Stortingets tilslutning til det rettslige grunnlaget som muliggjør en tydeliggjøring av PSTs etterretningsoppdrag, med korresponderende lovhjemmel, og hjemmel for behandling av åpent tilgjengelig informasjon. Alle de økonomiske og administrative konsekvensene er ikke endelig avklart, og anslagene over kostnader er usikre. Det foreslås ikke en bevilgning til formålet i regjeringens forslag til statsbudsjettet for 2023. Eventuelle videre forslag om anskaffelse og drift av tiltak vil legges frem for Stortinget i forbindelse med de årlige budsjettfremleggene.

Flere høringsinstanser, blant annet *Norges institusjon for menneskerettigheter (NIM), Medietilsynet, Advokatforeningen* og *Tekna* har pekt på at det er sentralt at EOS-utvalget har tilstrekkelige ressurser til å føre betryggende kontroll med PSTs bruk av de foreslåtte verktøyene. EOS-utvalget mener selv at en vedtakelse av de foreslåtte reglene vil kreve betydelig mer av utvalgets kontroll med PST.

EOS-utvalgets kontroll vil komme i tillegg til PSTs egen interne kontroll. PST har styrket sin internkontroll vesentlig det siste året, både i form av personell og verktøy, og departementet legger til grunn at dette vil bidra til å effektivisere også den kontrollen EOS-utvalget skal foreta. Dersom det legges til rette for kontroll i form av prosedyrer for notoritet ved innhenting, bruk og sletting av opplysninger, vil det forenkle den etterfølgende kontrollen. I tillegg må de tekniske systemene tilrettelegge for utvalgets kontroll.

Med den innramming av forslaget som foreslås i denne proposisjonen, legger departementet til grunn at kontroll med behandling etter den nye bestemmelsen vil kunne gjøres som en del av utvalgets alminnelige kontroll med PST, herunder kontroll med PSTs etterforskingssaker og forebyggende saker. Det kan imidlertid ikke utelukkes at forslaget vil medføre at EOS-utvalget vil motta flere begjæringer om kontroll. Departementet antar at dette vil kunne dekkes innenfor utvalgets tildelte budsjettrammer.

10 Merknader til de enkelte bestemmelsene

10.1 Til endringene i politiloven

Til § 17 a

Bestemmelsen endres slik at den angir PSTs oppgaver som innenlands etterretningstjeneste. PST skal etter bestemmelsen bidra til å sikre Norges suverenitet, territorielle integritet, demokratiske styreform og andre nasjonale sikkerhetsinteresser. Begrepet «nasjonale sikkerhetsinteresser» skal forstås på samme måte som definisjonen i sikkerhetsloven § 1-5 nr. 1. Dette skal gjøres ved å utarbeide analyser og etterretningsvurderinger om forhold i Norge som kan true disse interessene. Analysene og vurderingene skal gi grunnlag for beslutningsstøtte, det vil si å danne grunnlag for taktiske, operasjonelle og strategiske beslutninger. Ved at vurderingene skal gjelde forhold i Norge, avgrenses mandatet mot de forhold som hører under E-tjenestens ansvarsområde.

Til § 17 b

Som følge av at § 17 a endres til en bestemmelse som regulerer PSTs oppgaver som etterretningstjeneste, tydeliggjøres det i *overskriften* til bestemmelsen at § 17 b angir PSTs oppgaver som politiorgan.

10.2 Til endringene i politiregisterloven

Til § 3

I *annet ledd* tilføyes at PSTs etterretningsvirksomhet er omfattet av lovens virkeområde. Med etterretningsvirksomhet menes PSTs oppgaver som innenlands etterretningstjeneste slik disse er foreslått regulert i politiloven § 17 a. Behandling av opplysninger for disse oppgavene skal reguleres av politiregisterloven.

Til § 64

I *første ledd* tilføyes at PST kan behandle opplysninger for tjenestens etterretningsvirksomhet, jf. også endringene i § 3 og i politiloven § 17 a. I tillegg gjøres enkelte språklige justeringer som ikke innebærer realitetsendringer.

Tilføyelsen av *tredje ledd nytt nr. 6* er en følge av at PSTs oppgaver som innenlands etterretningstjeneste inntas i politiloven § 17 a. Ettersom nødvendighetskravet i politiregisterloven er knyttet til PSTs oppgaver slik de er definert i politiloven, må det gis en korresponderende hjemmel for å behandle opplysninger som er nødvendige for denne oppgaven. Dette gjør at PST kan behandle opplysninger utelukkende fordi de er nødvendige for utarbeidelse av analyser og etterretningsvurderinger.

Til ny § 65 a

Etter *første ledd* gis PST anledning til å behandle åpent tilgjengelig informasjon dersom det antas å være nødvendig for å utarbeide analyser og etterretningsvurderinger som nevnt i politiloven 17 a. Kravet om at det må «antas» å være nødvendig innebærer ikke et strengt sannsynlighetskrav, og terskelen for å kunne behandle opplysningene er lavere enn det alminnelige nødvendighetskravet i loven for øvrig. Det kreves ikke visshet om eller sannsynlighetsovervekt for at behandlingen er nødvendig. Det vil være tilstrekkelig at det er en rimelig, men ikke helt fjern, mulighet for at behandlingen er nødvendig.

I første ledd *annet punktum* presiseres at informasjon ikke er åpent tilgjengelig dersom tilgang krever aktivt fordekt opptreden eller forsering av passord eller lignende beskyttelsesmekanismer. Begrepet er dermed negativt avgrenset. Avgrensningen av hva som skal regnes som åpent tilgjengelig informasjon tilsvarer reguleringen i etterretningstjenesteloven § 6-2, og skal forstås på samme måte. Det sentrale vil være at opplysningene er tilgjengelige for allmennheten. Informasjon publisert på lukkede nettsteder eller private samtaler på chattetjenester, eposter eller annen kryptert eller privat kommunikasjon vil ikke være åpent tilgjengelig. Avgrensningen mot aktivt fordekt opptreden innebærer eksempelvis at informasjonen ikke er åpent tilgjengelig dersom en tjenesteperson må utgi seg for å være en annen, ikke-fiktiv

person og gjennom samhandling med mennesker oppnå tilgang til informasjon fra et forum på Internett. Det er ikke aktiv fordekt opptreden å betale vederlag for tilgang til informasjon som tilbys til allmennheten.

Første ledd *tredje punktum* åpner for at behandling i forbindelse med utarbeidelse av analyser og etterretningsvurderinger kan skje ved bruk av automatiserte analyseverktøy. Dette muliggjør at store mengder informasjon kan analyseres for å følge med på trender og utvikling over tid, noe som ikke er mulig med manuelle metoder. Bestemmelsen åpner for at det eksempelvis kan benyttes maskinlæringsmodeller som kan utvikle trendanalyser, grafer og sentimentanalyser, det vil si analyse av positive og negative holdninger, følelser og meninger. Automatiserte analyseverktøy kan ikke benyttes til forebygging og etterforsking. Det kan derfor ikke brukes verktøy basert på profilering for å identifisere enkeltindivider eller med det formål å predikere om enkeltpersoner i fremtiden, ut fra bestemte kriterier, vil antas å begå kriminalitet.

Etter første ledd *fjerde punktum* kommer kravene etter politiregisterloven § 6 om opplysningenes kvalitet mv. og § 7 om behandling av særlige kategorier av personopplysninger ikke til anvendelse for opplysninger som innhentes og lagres etter bestemmelsens første ledd. Dette innebærer at den enkelte opplysning ikke vil underlegges individuell vurdering, slik at disse bestemmelsene ikke er til hinder for at det kan lagres store mengder åpent tilgjengelig informasjon dersom det antas å være nødvendig for utarbeidelse av analyser og etterretningsvurderinger.

Kravene etter §§ 6 og 7 kommer heller ikke til anvendelse når behandlingen skjer ved hjelp av automatiserte analyseverktøy. Begrunnelsen for dette er at slike verktøy nettopp benyttes for å systematisere og analysere store mengder data, også data som inneholder opplysninger som ikke i seg selv er relevante.

For annen behandling i forbindelse med utarbeidelse av analyser og etterretningsvurderinger vil kravene etter §§ 6 og 7 gjelde fullt ut. Det innebærer blant annet at opplysninger som inngår i analyser og etterretningsvurderinger må være relevante og oppdaterte, og at særlige kategorier av opplysninger ikke kan inngå i slike analyser med mindre det er strengt nødvendig. Kravene i §§ 6 og 7 vil også gjelde fullt ut for bruk til forebygging og etterforsking.

Annet ledd angir at opplysningene skal være sperret. Sperring innebærer «*markering av lagrede opplysninger i den hensikt å begrense den fremtidige behandlingen av disse opplysningene*», jf. politiregisterloven § 2 nr. 10. Opplysninger som er sperret kan bare brukes til de konkret angitte formålene, og er ellers ikke ansett registrert. Sperrede opplysninger skal holdes atskilt fra opplysninger som ellers behandles hos PST.

Når opplysninger sperres, må det samtidig angis hvilke formål de sperrede opplysningene kan brukes til. Annet ledd *nr. 1 til 3* innebærer dermed en formålsbegrensning, ved at de sperrede opplysningene ikke kan brukes til andre formål enn de opplistede. Etter bestemmelsen kan opplysningene bare brukes til analyser og etterretningsvurderinger, opprettelse av eller i forebyggende sak eller til etterforsking av lovbrudd innenfor PSTs ansvarsområde.

Bruk til forebyggende sak og etterforsking forutsetter at vilkårene for opprettelse av slike saker er oppfylt, og kravene til behandling av opplysninger i den aktuelle sakstypen gjelder på vanlig måte. For etterforsking innebærer dette at det må være rimelig grunn til å undersøke om det foreligger et straffbart forhold som PST har i oppgave å etterforske, jf. straffeprosessloven § 224. Adgangen til å behandle opplysninger i straffesak følger reglene i straffeprosessloven, jf. politiregisterloven § 64 annet ledd. Kravet for opprettelse av forebyggende sak er at det er grunn til å undersøke om noen forbereder et lovbrudd som Politiets sikkerhetstjeneste har til oppgave å forebygge, jf. politiregisterloven § 64 tredje ledd nr. 1 bokstav a. I forebyggende sak kan det behandles opplysninger som har saklig tilknytning til saken, jf. politiregisterforskriften § 21-5 første ledd første punktum.

Dersom opplysningene tas i bruk til disse formålene, må de flyttes over i PSTs alminnelige systemer, og de vil ikke lenger være sperret. De vanlige behandlingsreglene i politiregisterloven og -forskriften vil gjelde for opplysningene, herunder reglene om utlevering og sletting.

Etter *tredje ledd* skal opplysninger som er sperret etter bestemmelsen slettes senest etter fem år, med en mulighet for å beslutte utsatt sletting for nærmere bestemte opplysninger eller datasett for inntil fem år av gangen dersom opplysningene etter en konkret vurdering fremdeles er nødvendige for utarbeidelse av analyser og etterretningsvurderinger. Dette vil eksempelvis kunne være tilfelle ved kartlegging av påvirkningsvirksomhet rettet mot valg over flere valgperioder. Opplysninger som er sperret etter bestemmelsen kan likevel ikke beholdes i mer enn 15 år, som vil danne den ytre rammen. Regelen gjelder kun for de sperrede opplysningene, og ikke for opplysninger som er

flyttet over i PSTs vanlige systemer. Adgangen til å beslutte utsatt sletting er ment å være en unntaksregel. Beslutningene må være skriftlige og begrunnet, slik at de kan kontrolleres av EOS-utvalget. Krav til skriftlighet og begrunnelse vil bli fastsatt i forskrift, jf. bestemmelsens fjerde ledd.

Etter *fjerde ledd* gir Kongen i forskrift nærmere regler om behandling av opplysninger etter bestemmelsen, herunder om utlevering, utsatt sletting, tilgangsbegrensning og kontroll. Oppregningen av hvilke forhold det kan gis forskrifter om er ikke uttømmende. Departementet tar blant annet sikte på å gi bestemmelser i forskriften som tydeliggjør krav til sporbarhet, kravene til beslutninger om å beholde opplysninger lenger enn slettefristen, regler om utlevering av sperrede opplysninger og at sperrede opplysninger skal slettes i form av tilintetgjøring. Videre vil departementet vurdere om det bør gis regler som ytterligere tydeliggjør at opplysninger som tas i bruk i konkrete saker må flyttes over i PSTs alminnelige registre, og at den videre behandlingen da vil følge de alminnelige behandlingsreglene i loven og forskriften.

Justis- og beredskapsdepartementet

t i l r å r :

At Deres Majestet godkjenner og skriver under et framlagt forslag til proposisjon til Stortinget om endringer i politiloven og politiregisterloven (PSTs etterretningsoppdrag og bruk av åpent tilgjengelig informasjon).

Vi HARALD, Norges Konge,

s t a d f e s t e r :

Stortinget blir bedt om å gjøre vedtak til lov om endringer i politiloven og politiregisterloven (PSTs etterretningsoppdrag og bruk av åpent tilgjengelig informasjon) i samsvar med et vedlagt forslag.

Forslag

til lov om endringer i politiloven og politiregisterloven (PSTs etterretningsoppdrag og bruk av åpent tilgjengelig informasjon)

I

I lov 4. august 1995 nr. 53 om politiet gjøres følgende endringer:

§ 17 a skal lyde:
§ 17 a *Oppgavene til Politiets sikkerhetstjeneste som innenlands etterretningstjeneste*

Politiets sikkerhetstjeneste skal utarbeide analyser og etterretningsvurderinger om forhold i Norge som kan true Norges suverenitet, territorielle integritet, demokratiske styreform og andre nasjonale sikkerhetsinteresser.

§ 17 b overskriften skal lyde:
Oppgavene til Politiets sikkerhetstjeneste som politiorgan

II

I lov 28. mai 2010 nr. 16 om behandling av opplysninger i politiet og påtalemyndigheten gjøres følgende endringer:

§ 3 annet ledd skal lyde:

Forvaltningsvirksomhet *og etterretningsvirksomhet* i Politiets sikkerhetstjeneste er likevel omfattet av loven.

§ 64 første ledd første punktum skal lyde:
Politiets sikkerhetstjeneste *kan behandle* opplysninger når det er nødvendig *for* politimessige formål, *etterretningsvirksomhet* og forvaltningsvirksomhet i tjenesten.

§ 64 tredje ledd nr. 4, 5 og nytt nr. 6 skal lyde:

4. er nødvendig for personkontroll eller akkreditering med de begrensninger som følger av *§ 67,*
5. er nødvendig for å dokumentere hvilken overskuddsinformasjon som er gjort tilgjengelig for andre*, eller*
6. *er nødvendig for å utarbeide analyser og etterretningsvurderinger som nevnt i politiloven § 17 a.*

Ny § 65 a skal lyde:
§ 65 a *Behandling av åpent tilgjengelig informasjon til etterretningsformål*

Politiets sikkerhetstjeneste kan behandle åpent tilgjengelig informasjon dersom det antas å være nødvendig for utarbeidelse av analyser og etterretningsvurderinger, jf. politiloven § 17 a. Informasjon er ikke åpent tilgjengelig dersom tilgang krever aktivt fordekt opptreden eller forsering av passord eller lignende beskyttelsesmekanismer. Behandling etter første punktum kan skje ved hjelp av automatiserte analyseverktøy. Når opplysningene etter dette leddet innhentes, lagres eller behandles ved hjelp av automatiserte analyseverktøy, kommer §§ 6 og 7 om krav til opplysningenes kvalitet og behandling av særlige kategorier av personopplysninger ikke til anvendelse.

Opplysninger som behandles etter første ledd skal være sperret, og kan bare brukes til følgende formål:

1. utarbeidelse av analyser og etterretningsvurderinger, jf. politiloven § 17 a
2. opprettelse av eller bruk i forebyggende sak, jf. § 64 tredje ledd nr. 1 bokstav a
3. etterforskning av lovbrudd som nevnt i politiloven § 17 b, jf. straffeprosessloven § 224

Opplysningene skal slettes senest etter 5 år. Sjefen for Politiets sikkerhetstjeneste eller den denne bemyndiger kan beslutte at nærmere angitte opplysninger skal beholdes i ytterligere 5 år av gangen, men ikke lenger enn 15 år totalt, dersom opplysningene etter en konkret vurdering fremdeles er nødvendige for formål som nevnt i annet ledd nr. 1.

Kongen gir i forskrift nærmere regler om behandling av opplysninger etter denne bestemmelsen, herunder om utlevering, utsatt sletting, tilgangsbegrensning og kontroll.

III

1. Loven gjelder fra den tid Kongen bestemmer. Kongen kan sette i kraft de enkelte bestemmelsene til ulik tid.

2. Kongen kan gi nærmere overgangsregler.

Bestilling av publikasjoner

Departementenes sikkerhets- og serviceorganisasjon
publikasjoner.dep.no
Telefon: 22 24 00 00

Publikasjonene er også tilgjengelige på
www.regjeringen.no

Trykk: Departementenes sikkerhets- og serviceorganisasjon – 12/2022