JUSTIS- OG BEREDSKAPSDEPARTEMENTET

Høringsnotat

Politiavdelingen
Dato: 7. oktober 2021
Saksnr: 21/4559
Høringsfrist: 7. januar 2022

Høring om endringer i politiloven og politiregisterloven mv. – PSTs etterretningsoppdrag og behandling av åpent tilgjengelig informasjon

Innhold

1 Innledning

Justis- og beredskapsdepartementet foreslår i dette høringsnotatet endringer i politiloven, politiregisterloven og politiregisterforskriften.

For det første foreslås det endringer i politiloven som lovfester og tydeliggjør PSTs oppdrag som innenlands etterretningstjeneste, og hva dette oppdraget innebærer. Det er i en rekke sammenhenger forutsatt og forventet at PST skal ha denne rollen allerede i dag, men oppdraget er ikke tilstrekkelig reflektert i dagens lovverk. Det foreslås også en klar hjemmel i politiregisterloven for at PST kan behandle opplysninger som er nødvendige for dette formålet.

Det foreslås i tillegg en ny bestemmelse i politiregisterloven som åpner 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. Begrunnelsen for endringsforslaget er at det etter departementets syn er nødvendig å åpne for denne typen behandling for at PST skal kunne ivareta etterretningsoppdraget og oppfylle forventningen om at de skal «følge med» på internett. Forslaget vil bidra til at PST kan avdekke ukjente trusselaktører, kartlegge utviklingen i trusselbildet og oppdage nye fenomener som kan medføre nye trusler. Det understrekes at forslaget ikke vil innebære en generell adgang til å følge med på enkeltpersoners aktivitet på internett. I tillegg foreslås det å åpne for at de lagrede opplysningene kan brukes i forebyggende sak og i etterforskingen av straffbare handlinger innenfor PSTs ansvarsområde.

Med åpent tilgjengelig informasjon menes informasjon som er allment tilgjengelig for offentligheten. Det omfatter for eksempel nettavisartikler, åpne offentlige registre, åpne diskusjoner i sosiale medier, kommentarfelt, blogger mv. Forslaget åpner derfor ikke for massenedlasting av informasjon som ikke er åpent tilgjengelig, for eksempel informasjon publisert på lukkede nettsteder eller privat

kommunikasjon, som private samtaler fra chattetjenester, eposter eller annen kryptert eller privat kommunikasjon.

Som en sentral sikkerhetsmekanisme foreslås det at den lagrede informasjonen skal *sperres*. Dette innebærer at opplysningene kun 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, og tilgang til opplysningene skal bare gis til personer som har fått særskilt bemyndigelse. Bruk av opplysningene skal kunne spores, for derved å kunne avdekke eventuell urettmessig bruk og sikre at EOS-utvalget kan føre kontroll med behandlingen. Opplysningene skal slettes senest etter 15 år.

2 Bakgrunn og behovet for endringer

2.1 Tydeliggjøring av PSTs etterretningsoppdrag

Dagens bestemmelser om PSTs oppdrag i politiloven ble vedtatt rundt årtusenskiftet. Siden den gang er trusselbildet vesentlig endret. Norges sikkerhetspolitiske omgivelser er i betydelig endring, påvirket av den teknologiske og samfunnsmessige utviklingen, jf. Prop. 14 S (2020-2021) *Evne til forsvar – Vilje til beredskap – Langtidsplan for forsvarssektoren* side 19 til 23 og Meld. St. 5 (2020-2021) *Samfunnssikkerhet i en usikker verden* side 23. Trusselbildet i dag er mer sammensatt og komplekst enn før. Samtidig bidrar den teknologiske og samfunnsmessige utviklingen til at mengden informasjon som genereres har økt betydelig. Dagens informasjonssamfunn kan blant annet kjennetegnes ved dets omløpshastighet, informasjonsmengde og kompleksitet gjennom sammenveving av teknologi og samfunn.

En annen følge av disse endringene er at forhold i utlandet i større grad enn tidligere får betydning for nasjonale forhold. Samtidig er grensen mellom utenlands og innenlands trusler redusert, og skillet mellom stats- og samfunnssikkerheten er blitt mindre tydelig. Det er derfor et økt behov for formidling av rettidig, relevant og pålitelig etterretning til landets øverste beslutningstakere, som danner grunnlag for strategiske beslutningsprosesser for å ivareta nasjonale sikkerhetsinteresser. Utviklingen stiller derfor større krav om en tydelig nasjonal innenlands etterretningstjeneste.

Det er en økende forventning om at PST i større grad skal kunne vurdere sannsynlig fremtidig trusselutvikling i Norge, og hvilke trusselaktører vi vil stå overfor her hjemme i fremtiden. Det er også en forventning om at PST på mer generelt grunnlag skal kunne beskrive utviklingen i trusselbildet og endringer blant trusselaktører i samfunnet innenfor PSTs ansvarsområde. Denne forventningen er det vanskelig for tjenesten å oppfylle når den ikke er gitt et klart mandat for å utføre oppgaven, og regelverket heller ikke åpner for å behandle opplysninger kun for dette formålet.

At PSTs oppgave som innenlands etterretningstjeneste, og hva denne oppgaven innebærer, ikke fremgår eksplisitt av regelverket, gjør også at PSTs og Etterretningstjenestens (E-tjenestens) mandat ikke fullt ut utfyller hverandre.

E-tjenesten har ansvaret for utenlandsetterretningen, og skal i den forbindelse innhente og analysere informasjon om utenlandske forhold som kan bidra til å avdekke og motvirke blant annet trusler mot Norges selvstendighet og sikkerhet,

territorielle integritet og politiske og økonomiske handlefrihet, alvorlige trusler mot samfunnssikkerheten i Norge og fremmed etterretningsvirksomhet, jf. lov om Etterretningstjenesten § 3-1. Som hovedregel skal E-tjenesten ikke drive informasjonsinnhenting på norsk territorium, jf. lov om Etterretningstjenesten § 4-1, og innhentingen er avgrenset til å avdekke og motvirke trusler mot Norge fra utlandet.

PST har i dag ikke tilsvarende muligheter som E-tjenesten til å bidra med rettidig og relevant innenlandsetterretning. Ved at PSTs oppdrag etter politiloven i hovedsak er beskrevet som forebygging og etterforsking av konkret angitte straffbare handlinger, er tjenestens mulighet til behandle informasjon for å bidra med generelle etterretningsvurderinger og analyser knyttet til trender og utvikling i trusselbildet, begrenset.

Departementet vil derfor foreslå at det gis en klar hjemmel for PSTs etterretningsoppdrag i politiloven, og at det i tillegg gis en hjemmel i politiregisterloven for behandling av opplysninger for dette formålet. Dette er beskrevet nærmere nedenfor under punkt 5.1.

2.2 Utvidet bruk av åpent tilgjengelig informasjon

Den digitale hverdagen har medført store endringer i trusselbildet. 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. Den teknologiske og samfunnsmessige utviklingen medfører dessuten at trusselaktørene i økende grad flytter sin aktivitet fra det fysiske til det digitale rom. Dette innebærer 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.

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 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 om informasjon innhentet ved bruk av åpne kilder ble 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 i det høyreekstreme trusselbildet etter 22. juli 2011 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 trusselbildet. I PSTs åpne trusselvurdering for 2021 uttales det blant annet:

«Trusler i det digitale rom vil fortsette i 2021. Den digitale trusselen fra statlige aktører er alvorlig, og ingenting tyder på at den blir redusert. Samtidig ser vi en utvikling der ekstreme grupper og potensielle terrorister formes og påvirkes av propagandaen fra digitale nettverk. Arbeidet med å identifisere, avdekke og forebygge trusler i det digitale rom griper dermed inn i de fleste av PSTs oppgaver.»

I tillegg har PST i temarapporten *Dataspill, selfie-jihad og livestreaming av terrorangrep: Hvordan ekstreme digitale nettverk påvirker terrortrusselen i Vesten og Norge*, 12. mars 2021, pekt på at terrortrusselen de kommende årene hovedsakelig vil komme fra enkeltpersoner, der mange vil ha tilknytning til ekstreme digitale nettverk. Nye organisasjoner og nye terroraksjoner vil kunne springe ut av slike nettverk. Dette skaper nye utfordringer for arbeidet med å identifisere og avdekke terror.

Det er ikke tvilsomt at PST allerede i dag har anledning til å behandle informasjon fra åpne kilder når behandlingen er knyttet til tjenestens oppdrag, slik dette er definert i politiloven, så lenge vilkårene for behandling av opplysningene etter politiregisterloven er oppfylt. En tydeliggjøring av PSTs etterretningsoppdrag i politiloven vil som nevnt under punkt 2.1, samtidig legge til rette for at alle typer informasjon, herunder informasjon fra åpne kilder, vil kunne behandles til rene etterretningsformål.

For å kunne kartlegge eller «følge med» på utviklingen i digitale trusler over tid, vil det imidlertid kunne være nødvendig for tjenesten å lagre, systematisere og analysere større mengder åpent tilgjengelig informasjon. Politiregisterlovens alminnelige regler om behandling av opplysninger åpner ikke for denne typen behandling.

Departementet foreslår derfor en endring i politiregisterloven som åpner for at PST i større grad enn i dag kan nyttiggjøre seg åpent tilgjengelig informasjon. Dette vil bidra til at tjenesten sikres gode nok virkemidler til å vurdere sannsynlig fremtidig trusselutvikling og hvilken risiko slike trusler innebærer. Forslaget er nærmere beskrevet under punkt 5.2 nedenfor.

3 Gjeldende rett

3.1 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. Etter denne bestemmelsen skal PST blant annet forebygge og

etterforske følgende straffbare handlinger som kan true rikets sikkerhet: Overtredelser av straffeloven kapittel 17 og § 184 og 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, som er gitt med hjemmel i politiloven § 29, fastsetter nærmere regler om PSTs oppgaver og virksomhet, jf. instruksen § 1. I § 5 første ledd fremgår at tjenesten skal utføre sine forebyggende oppgaver ved blant annet å «innhente, bearbeide, analysere og utveksle informasjon» i samsvar med fastsatte prioriteringer. I § 6 første ledd fremgår 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»*.

3.2 Politiregisterloven og politiregisterforskriften

Politiregisterloven og politiregisterforskriften regulerer politiets og påtalemyndighetens behandling av opplysninger. Behandling av opplysninger er etter definisjonen i politiregisterloven § 2 nr. 2 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. Siden PST er en del av politiet er politiregisterloven gitt anvendelse for PST selv om direktivets virkeområde ikke omfatter de nasjonale etterretningstjenestene, jf. artikkel 2 nr. 3 a. Det er likevel gitt en rekke særbestemmelser for tjenesten. 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 mest markante forskjellene i forhold til politiet for øvrig finnes i §§ 64, 66 og 68 om henholdsvis nødvendighetskravet, informasjonsplikt, innsyn og tilsyn. For PSTs behandling av opplysninger er nødvendighetskravet direkte knyttet til politiloven §§ 17 b, 17 c og 17 d, som beskriver PSTs arbeidsoppgaver. 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. Utover dette gjelder politiregisterlovens bestemmelser også for PST.

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. Sperrede opplysninger kan bare brukes til de formål som gjorde at opplysningen ikke ble slettet, jf. § 52. Dette innebærer at det må særskilt angis hvilke formål de sperrede opplysningene kan brukes til. Videre følger det av politiregisterforskriften § 15-2 annet ledd at opplysninger som er sperret skal holdes atskilt. Tilgang til opplysninger som er sperret skal begrenses til så få personer som mulig, og bare gis til personer som har fått særskilt bemyndigelse.

I politiregisterforskriften er det gitt supplerende bestemmelser til politiregisterloven. PSTs behandling av opplysninger er regulert i del 6 i forskriften. 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 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. Kapittel 22 gir regler om informasjonsplikt, innsyn, retting, sperring og sletting. Kapittel 23 gjelder informasjonssikkerhet og internkontroll.

Ved forskrift 3. september 2021 nr. 2658 ble det vedtatt en rekke forenklinger, presiseringer og klargjøringer i politiregisterforskriften del 6. Endringene trer i kraft 1. november 2021.

3.3 Lov om Etterretningstjenesten

Lov 19. juni 2020 nr. 77 om Etterretningstjenesten (etterretningstjenesteloven) regulerer E-tjenestens virksomhet og oppgaver. I § 2-1 første ledd første punktum fremgår det eksplisitt at E-tjenesten er Norges nasjonale utenlandsetterretningstjeneste. Tjenestens oppgaver er angitt i kapittel 3, der det blant annet i § 3-1 er angitt 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 en mulighet til forlengelse i inntil 5 år av gangen dersom vesentlige

hensyn tilsier at sletting utsettes. 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 annet punktum at informasjon ikke er åpent tilgjengelig dersom tilgang krever aktiv fordekt opptreden eller forsering av passord eller lignende beskyttelsesmekanismer. I merknadene til bestemmelsen i Prop. 80 L (2019-2020) kapittel 17 på side 208 fremgår det: *«Innhenting av informasjon fra åpne kilder faller normalt innenfor den alminnelige handlefriheten, og krever ikke hjemmel i lov. Etter omstendighetene kan innhenting fra åpne kilder om en bestemt person likevel få et slikt omfang at det kan reises spørsmål om den utgjør et inngrep overfor vedkommende. For å unngå tvil om lovligheten av metoden foreslås det derfor å lovfeste den.»* Det er i Prop. 80 L (2019-2020) punkt 10.5.3.understreket at man i lovarbeidet med etterretningstjenesteloven ikke tar stilling til spørsmålet om lovfesting av ulovfestede politimetoder.

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. Etterretningstjenesteloven kapittel 7 og 8 trer i kraft 1. januar 2022, med unntak av § 7-3 om kravene som stilles til beslutningen om å pålegge ekomtilbydere tilrettelegging, jf. kongelig resolusjon 26. august 2021 nr. 2581.

3.4 Grunnloven og internasjonale forpliktelser

3.4.1 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 tillegg finnes det forskjellige internasjonale regelsett som danner rammer for norsk lovgivning. Av særlig betydning i denne sammenheng er Den europeiske menneskerettskonvensjonen av 4. november 1950 (EMK), som gjennom menneskerettsloven av 21. mai 1999 nr. 30 er gjort til norsk lov, og som går foran annen norsk lovgivning ved motstrid. Retten til privatliv beskyttes også av FNs konvensjon om økonomiske, sosiale og kulturelle rettigheter (SP) artikkel 17.

Forslagene i dette høringsnotatet gjelder masseinnhenting og behandling av informasjon fra åpne kilder, eksempelvis internett, avisartikler og åpne registre, til bruk for etterretningsformål, herunder beskrivelse av fenomener, trender og utvikling. I det følgende vil det bli belyst i hvilken grad slik behandling av opplysninger berøres av de nevnte bestemmelsene om vern av privatlivet.

3.4.1.1 *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»*.

Etter ordlyden i Grunnloven § 102 er det ikke adgang til å gjøre unntak 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 etter Grunnloven § 102 kan være lovlig, 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. 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.

Når det gjelder behandling av *offentlig tilgjengelig informasjon*, er det flere avgjørelser fra EMD som gir anvisning på at innsamling av slik informasjon vil kunne innebære et inngrep i EMK artikkel 8. 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 tilgjengelig materiale 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 anses å utgjøre et inngrep i privatlivet etter EMK artikkel 8 nr. 1, selv om informasjonen er offentlig tilgjengelig.

3.4.1.2 *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 overvåkning 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 i stor grad fra hemmelig overvåking av kommunikasjon i transitt og andre former for hemmelig overvåking. Som følge av dette har de kravene som er oppstilt i dommene nedenfor begrenset overføringsverdi for forslaget i dette høringsnotatet. Departementet gjør likevel kort rede for enkelte dommer om masseovervåkning av kommunikasjon i transitt.

EMDs nyeste avgjørelser om slik masseovervåkning er avgjørelsene i storkammersakene *Big Brother Watch and Others mot Storbritannia* og *Center för Rättvisa mot Sverige*, begge fra 25. mai 2021. EMD la i disse sakene til grunn at masseinnsamling er en gradvis prosess, der inngrepet i individets rettigheter etter artikkel 8 tiltar underveis i prosessen, se *Big Brother Watch and Others 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 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 på slutten av prosessen, når innholdet i kommunikasjonen blir nærmere undersøkt, se avsnitt 330.

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 en generell og udifferensiert innsamling og lagring av slike opplysninger ville være i strid med grunnleggende rettigheter og EUs kommunikasjonsverndirektiv. Dommen åpner imidlertid for ikke-målrettet innhenting av trafikk- og lokaliseringsdata dersom lagringen begrenses til det som er strengt nødvendig basert på en reell trussel avgrenset til angitte kategorier av data, hvilke kommunikasjonsmidler som benyttes, de berørte personer og varigheten av innsamlingen og lagringstiden.

3.4.1.3 *Krav til lovhjemmel og proporsjonalitet*

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 det videre 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 ivareta 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 anses forholdsmessig, må vurderes konkret. EMD har lagt til grunn at statene har en nokså vid skjønnsmargin med hensyn til 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 overvåkning 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 her. 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 videre at moderne kommunikasjonsformer og forandringer i kommunikasjon krever at etterforskningsverktøyene 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 de lagrede dataene, men også reglene om 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 overvåkning 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 vedrørende kontrollmekanismer knyttet til mer vesentlige inngrep i privatlivet hadde begrenset overføringsverdi til saker der inngrepet var mindre. I avsnitt 103 ble 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 utformes slik at innholdet relativt presist gir borgerne mulighet til forutsigbarhet. Videre må det foreligge sikkerhetsmekanismer som hindrer vilkårlighet og myndighetsmisbruk. Departementet kommer nærmere tilbake til hvordan dette er vurdert nedenfor under punkt 5.2.

3.4.2 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 noe sterkere vern av ytringsfriheten enn det som følger av EMK artikkel 10, konsentreres fremstillingen om sistnevnte, som lyder (i norsk oversettelse):

«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 følgende.

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 3.4.1.2 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 såfremt behandlingen av informasjon knyttet til 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.

3.4.3 Kommunikasjonsverndirektivet

Europaparlaments- og rådsdirektiv 2002/58/EF av 12. juli 2002 om behandling av personopplysninger og personvern i sektoren for elektronisk kommunikasjon (kommunikasjonsverndirektivet), er gjennomført i norsk rett gjennom ekomloven med forskrifter. Det følger av direktivet artikkel 5 nr. 1 at medlemsstatene plikter å sikre fortrolighet for kommunikasjon som foregår via offentlige kommunikasjonsnett og offentlig tilgjengelige elektroniske kommunikasjonstjenester, samt fortrolighet for trafikkopplysninger knyttet til slik kommunikasjon. Videre skal medlemsstatene forby enhver annen person enn brukerne å avlytte, oppfange, lagre eller på andre måter oppfange eller overvåke kommunikasjonen og tilhørende trafikkopplysninger uten samtykke fra brukeren, med mindre dette er tillatt i henhold til lov, i samsvar med artikkel 15 nr. 1.

Kommunikasjonsverndirektivet kommer ikke til anvendelse for de tilfeller der det ikke kreves bistand fra ekomtilbyderne for å få tilgang til kommunikasjonen. Ettersom forslaget her innebærer innhenting av åpent tilgjengelig informasjon i det digitale rom, noe PST vil kunne gjøre uten bistand fra ekomtilbyderne, omtales ikke direktivet nærmere.

4 Andre lands rett

4.1 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.

4.2 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.

4.3 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 der formålet er 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).

4.4 Andre land

I flere vestlige land som Norge kan sammenlignes med, 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).

5 Departementets vurderinger

5.1 Regulering av PSTs etterretningsoppdrag

5.1.1 Behovet for tydeliggjøring

I tillegg til å forebygge og etterforske straffbare forhold som nevnt i politiloven § 17 b, har PST rollen som Norges innenlands etterretningstjeneste. Dette fremgår ikke direkte av politiloven, men kan til dels utledes av blant annet politiloven § 17 c, hvor det fremgår at den sentrale enhet i PST (DSE) skal utarbeide trusselvurderinger til bruk for politiske myndigheter, og av instruks for Politiets sikkerhetstjeneste §§ 5 og 6, jf. omtalen i punkt 3.1 over.

At PST også har oppgaver av mer etterretningspreget karakter, er forutsatt i en rekke ulike sammenhenger. 22. juli-kommisjonen viser på side 381 til at:

«En sikkerhetstjenestes evne til å løse sine oppgaver står og faller på fokuserte etterretningsbehov og evnene til godt etterretningsarbeid og systematisk innhenting, bearbeiding og strategisk analyse av informasjon. En god etterretningsprosess forutsetter at tjenesten er i stand til 'å tenke utenfor boksen', det vil si at den etablerte prosessen utfordres og forstås dynamisk.»

I Prop. 80 L (2019-2020) punkt 8.4.4.1 er det vist til at samordningsbestemmelsen i etterretningstjenesteloven § 4-3, som pålegger E-tjenesten å innhente samtykke

fra PST til innhenting i Norge i gitte tilfeller, *«understreker at det er PST som er landets innenlands sikkerhets- og etterretningstjeneste, med det primære ansvaret for å innhente informasjon om trusselaktører i Norge»*.

I den eksterne gjennomgangen av Politiets sikkerhetstjeneste (Traavikutvalget), avgitt 1. desember 2012, er det på side 23 vist til at *«Den viktigste oppgaven for en sikkerhetstjeneste er informasjonsinnhentings- og informasjonshåndteringsprosessen, også omtalt som etterretningsvirksomheten.»*

I forskrift 3. september 2021 nr. 2658 om endringer i politiregisterforskriften er det vedtatt å innta «etterretning» i politiregisterforskriften § 20-2 om formålet med behandling av opplysninger i PST. I den kongelige resolusjonen er det uttalt følgende om forslaget:

«Når det gjelder etterretningsvirksomhet ble det [i høringsnotatet] vist til at selv om begrepet «etterretning» ikke fremgår uttrykkelig av politiloven, er det ikke noen tvil om at etterretning er en sentral del av PSTs virksomhet. PST er i dag en politi- og sikkerhetstjeneste med ansvar for å beskytte Norge innenlands. PSTs mandat etter politiloven § 17 b er å forebygge og etterforske de mest alvorlige truslene mot landets sikkerhet. I denne bestemmelsen, som angir tjenestens oppgaver, ligger en iboende forventning om at PST blant annet skal verne om Norges selvstendighet og andre grunnleggende, nasjonale interesser samt forebygge terrorhandlinger. Videre er etterretning en grunnleggende forutsetning for å kunne utarbeide trusselvurderinger til bruk for politiske myndigheter, jf. politiloven § 17 c. På denne bakgrunn fant departementet det ønskelig at denne sentrale delen av PSTs virksomhet gjenspeiles uttrykkelig i forskriften.»

Selv om det altså er forutsatt at PST skal drive med etterretning innenfor sitt mandat, er dette i begrenset grad reflektert i regelverket. Samtidig er det en økende forventning om at PST skal kunne forutse fremtidig trusselutvikling og hvilke trusselaktører vi står overfor, og på mer generelt grunnlag kunne beskrive denne utviklingen, jf. punkt 2.1.

PSTs behandling av opplysninger er regulert i politiregisterloven. Reglene i § 64, som lister opp formålene som PSTs behandling av opplysninger skal ivareta, er knyttet til oppgavene som er angitt i politiloven. Når det ikke fremgår av politiloven at PST skal drive med etterretning, kan tjenesten dermed heller ikke uten videre behandle opplysninger kun for dette formålet. Dette gjør at PST har begrensede muligheter til å jobbe med enkelte typer trusler, 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 må derfor i dag primært baseres på informasjon som er innhentet til andre formål, herunder fra konkrete saker, forskning og informasjon fra samarbeidende tjenester, der det foreligger en klar hjemmel for å behandle opplysningene. Dette innebærer en risiko for etterretningssvikt da vurderingene kan være basert på et utilstrekkelig etterretningsgrunnlag, enten fordi informasjonen kan være uriktig, ikke tilstrekkelig verifisert eller fordi den er mangelfull.

Etter departementets syn er det derfor god grunn til å tydeliggjøre denne delen av tjenestens virksomhet i politiloven og gi en klar hjemmel for behandling av opplysninger for dette formålet i politiregisterloven.

5.1.2 Forslag til endringer

I dag fremgår det av politiloven § 17 a kun at PST er et eget politiorgan. At tjenesten har en rolle ut over dette kommer ikke i tilstrekkelig grad frem. Departementet foreslår at det skal fremgå eksplisitt av politiloven § 17 a at PST i tillegg er Norges nasjonale innenlands etterretningstjeneste. Dette vil kunne bidra til at E-tjenestens og PSTs mandater utfyller hverandre bedre. Som omtalt i punktet over er det allerede lagt til grunn at PST har denne funksjonen, slik at denne endringen ikke i seg selv innebærer realitetsendringer.

Samtidig bør det tydeliggjøres hva som ligger i rollen som innenlands etterretningstjeneste. I den forbindelse er det verdt å merke seg at «etterretning» ikke er et entydig rettslig begrep med et klart innhold. I politiets etterretningsdoktrine er etterretning definert som *«en styrt prosess, bestående av systematisk innsamling, analyse og vurdering av informasjon om personer, grupper og fenomener for å danne grunnlag for beslutninger»*. I Forsvarets etterretningsdoktrine (2021) er etterretning definert som *«resultatet av statlig sanksjonert innhenting, analyse og vurdering av data og informasjon, som er generert åpent eller fordekt og utarbeidet for å gi fortrinn i beslutningsprosesser»*.

«Etterretning» benyttes både om en arbeidsprosess, et produkt som kommer ut av prosessen og om organisasjonen som utøver etterretning. Arbeidsprosessen kan beskrives som en styrt prosess, bestående av systematisk innhenting, analyse og vurdering av informasjon om aktører som kan utgjøre en trussel. Formålet med etterretning er å beskrive trusselen, for å kunne gi grunnlag for beslutningstakeres vurdering og prioritering av hvilke trussel- og sårbarhetsreduserende tiltak som bør iverksettes. Hovedformålet kan med andre ord beskrives som *varsling* og *beslutningsstøtte* til beslutningstakere.

Departementet mener etter dette at det bør gis en mer konkret beskrivelse av hva det innebærer å være landets innenlands etterretningstjeneste.

Den delen av tjenestens etterretningsvirksomhet som knytter seg til straffbare forhold som angitt i politiloven § 17 b, kan anses å utgjøre en del av PSTs forebyggende virksomhet. Forebygging kan skje både i vid og snever forstand, også i form av innhenting, bearbeiding og analyse av informasjon med sikte på kriminalitetsbekjempelse. Dette betegnes gjerne som *kriminaletterretning*.

Samtidig vil det gå en grense for når man reelt sett kan si at man forebygger straffbare forhold. Dersom hensikten er å utarbeide analyser om en fremtidig trusselutvikling, som skal danne grunnlag for prioriteringer fra overordnede myndigheter, kan dette neppe betegnes som forebygging. En for vid tolkning vil kunne medføre en uønsket utvanning av forebyggingsbegrepet.

Etter departementets vurdering bør det derfor tydeliggjøres at PST skal drive etterretningsvirksomhet i tilknytning til de straffbare forhold som tjenesten skal forebygge og etterforske etter politiloven § 17 b første ledd. Endringen vil 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. Eksempelvis må tjenesten etter mottak av tips om at det innenfor enkelte miljøer foregår rekruttering til terrorhandlinger, kunne kartlegge om det er personer innenfor disse miljøene som igjen forsøker å rekruttere personer til å begå terrorhandlinger. Endringen vil ikke utvide tjenestens mandat, men vil bidra til en synliggjøring av denne delen av tjenestens oppgaveløsning.

Etter departementets syn er det imidlertid behov for å tydeliggjøre PSTs etterretningsoppdrag også utover dette. PST skal etter politiloven § 17 c nr. 1 utarbeide trusselvurderinger. Som omtalt i punkt 5.1.1 utarbeides disse trusselvurderingene primært på bakgrunn av informasjon som allerede er innhentet til andre formål. Departementet mener at det bør åpnes for at PSTs trusselvurderinger kan baseres på et bredere informasjonstilfang, for å kunne imøtekomme behovene for beslutningsstøtte. Som ledd i dette bør tjenesten derfor etter departementets vurdering kunne drive etterretningsvirksomhet innenfor sitt ansvarsområde for å kartlegge trender og utviklingstrekk med sikte på å utarbeide analyser og etterretningsvurderinger. Dette bør også gå tydelig frem av lovbestemmelsen.

Slike trusselvurderinger kan eksempelvis omfatte kartlegging og vurdering av uønsket 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 er 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. Dette vil gjøre at PST i større grad enn i dag kan bidra til at norske myndigheter får rettidig og relevant informasjon om trusler i Norge, på samme måte som E-tjenesten innenfor sitt mandat bidrar med slik informasjon om utenlandske forhold. Ofte vil E-tjenestens vurderinger av utenlandske forhold og trusler mot Norge fra utlandet måtte vurderes i lys av nasjonale forhold. Herunder må det vurderes hvordan en eventuell trussel vil kunne materialisere seg i Norge. Da må PST kunne følge opp informasjonen innenfor sitt mandat.

Det bes særlig om høringsinstansenes syn på formuleringen av etterretningsoppdraget.

Som omtalt over er nødvendighetskravet for PSTs behandling av opplysninger knyttet til oppgavene etter politiloven. Som følge av endringen foreslås det derfor også å tilføye et nytt nr. 6 i politiregisterloven § 64 tredje ledd, slik at PST kan behandle opplysninger når det er nødvendig for etterretningsvirksomheten, jf. politiloven § 17 b fjerde ledd, dvs. når det er nødvendig for å kartlegge trender og utviklingstrekk som har tilknytning til PSTs oppgaver.

5.2 Behandling av åpent tilgjengelig informasjon til etterretningsformål – endringer i politiregisterloven og politiregisterforskriften

5.2.1 Noen innledende merknader

Politiregisterloven er – på lik linje med all annen personvernlovgivning – basert på at opplysninger bare kan behandles dersom dette er nødvendig og relevant for nærmere angitte formål. I tillegg er det gitt en rekke regler om den nærmere behandlingen av opplysningene og hvilke krav som stilles til opplysningenes kvalitet.

I politiregisterloven skilles det mellom behandling av opplysninger i og utenfor straffesaker. For behandling av opplysninger i straffesaker er det straffeprosessloven som angir formålet og rammene for behandlingen. For

behandling av opplysninger utenfor straffesaker er det imidlertid politiregisterloven selv som angir formålet og rammene for behandlingen.

For PSTs behandling av opplysninger er bildet noe mer sammensatt. Når det gjelder behandling av opplysninger *i straffesaker* gjelder de samme reglene for PST som for det øvrige politiet. Forslaget i dette høringsnotatet vil således ikke medfører noen endringer for denne behandlingen. Når det gjelder behandling av opplysninger *utenfor straffesaker* er det for PST gitt en rekke særregler i politiregisterloven kapittel 11. For PSTs del er formålet med behandlingen etter politiregisterloven § 64 i hovedsak direkte knyttet til PSTs oppgaver slik de er beskrevet i politiloven, jf. omtalen i punkt 3.1 over. Som følge av dette må endringer i PSTs oppgaver i politiloven som tidligere nevnt også gjenspeile seg i politiregisterloven § 64.

En utfordring er imidlertid at behandling av store mengder åpent tilgjengelig informasjon for etterretningsformål ikke vil være mulig innenfor de tradisjonelle behandlingsreglene. Disse reglene er tuftet på at krav til behandling er knyttet til den enkelte opplysningen. Når det nå foreslås å åpne for registrering av større mengder offentlig tilgjengelig informasjon uten at det foretas noen nærmere vurdering av den enkelte opplysningen, innebærer dette noe nytt. Politiregisterlovens alminnelige regler for behandling av opplysninger passer ikke for denne typen virksomhet.

Departementet ser at det er knyttet betydelige personvernmessige betenkeligheter til å gi PST hjemmel til å samle inn og behandle store mengder informasjon fra åpne kilder. Dette vurderes imidlertid som nødvendig for å sette tjenesten i stand til å ivareta oppgaven som innenlands etterretningstjeneste på en forsvarlig måte. For å demme opp for de personvernmessige betenkelighetene, er det viktig å etablere tilstrekkelig gode sikkerhetsmekanismer. I det følgende utdypes derfor både behovet for å kunne behandle åpent tilgjengelig informasjon, og hvilke tiltak som etter departementets oppfatning er egnet til å redusere de personvernmessige betenkelighetene som forslaget innebærer.

Etablering av tilstrekkelige sikkerhetsmekanismer er også nødvendig for å ivareta de rettslige krav som følger av Grunnloven § 102 og EMK artikkel 8. Som omtalt i punkt 3.4.1 over vil lagring av offentlig tilgjengelig informasjon om enkeltmennesker kunne utgjøre et inngrep i retten til respekt for privatlivet, særlig der innhentingen er systematisk og informasjonen lagres over tid. Departementet legger derfor til grunn at ordningen som foreslås her i praksis vil medføre et inngrep i retten til privatliv. I tillegg til å gi en klar hjemmel for behandlingen, må det da etableres klare rammer for behandlingen slik at inngrepet overfor den enkelte ikke blir større enn nødvendig. Det må også etableres sikkerhetsmekanismer for å unngå misbruk, og det må sikres at EOS-utvalget kan føre tilstrekkelig kontroll med bruken. Omfanget av sikkerhetsmekanismer og kontroll må vurderes i lys av inngrepets alvor. Det er i den sammenheng sentralt at det er tale om offentlig tilgjengelig informasjon som ikke innhentes ved bruk av tvangsmidler eller gjennom skjult overvåkning. Dette omtales nærmere i punktene nedenfor.

5.2.2 Behovet for endringer og konsekvenser av forslagene

Som omtalt i punkt 2.2 er det 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. Internett er en stor og uoversiktlig arena, som mange trusselaktører benytter seg av og som er i kontinuerlig endring. 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.

For at PST skal kunne oppfylle oppdraget som innenlands etterretningstjeneste er det derfor etter departementets syn behov for å åpne for at PST kan lagre, systematisere og analysere åpent tilgjengelig informasjon som ledd i tjenestens etterretningsvirksomhet. Dette vil gjøre at PST i større grad vil kunne kartlegge utvikling, avdekke nye trender i trusselbildet og forutse fremtidige trusler i Norge. Det vil 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.

Departementet ser at slik bruk av åpent tilgjengelig informasjon innebærer at PST vil kunne lagre og behandle svært store mengder informasjon, hvorav mye av informasjonen vil være av mindre interesse for PSTs oppgaveløsning. Det er på det rene at forslaget vil innebære behandling av en slik art at det vil utgjøre et inngrep i privatlivet, jf. omtalen i punkt 3.4.1 og 5.2.1 over. Det er også en risiko for at et slikt tiltak 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 vil imidlertid dette tiltaket være en grunnleggende forutsetning for at PST skal kunne ivareta oppgaven med å kartlegge trender og utviklingstrekk og utarbeide analyser og etterretningsvurderinger av betydning for bekjempelsen av den alvorlige kriminaliteten som tjenesten har et særskilt ansvar for, herunder for å kunne utarbeide trusselvurderinger innenfor PSTs ansvarsområde. Holdt opp mot dette, og sett hen til sikkerhetsmekanismene som er nærmere beskrevet nedenfor, kan risikoen for en eventuell nedkjølende effekt etter departementets syn ikke tillegges avgjørende vekt. På samme vis som inngrepet i privatliv vil kunne anses rettferdiggjort etter EMK artikkel 8 nr. 2, legger 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 anses også tilstrekkelig ivaretatt.

5.2.3 Hva menes med åpent tilgjengelig informasjon?

Departementet understreker at forslaget her er begrenset til *åpent tilgjengelig informasjon*. Det innebærer at for eksempel informasjon publisert på lukkede nettsteder eller private samtaler på chattetjenester, eposter eller annen kryptert eller privat kommunikasjon, ikke omfattes. Forslaget skiller seg dermed vesentlig fra tilrettelagt innhenting, bruk av skjulte tvangsmidler og andre inngripende overvåkingsmetoder. Som følge av dette har kravene som er oppstilt i dommene

som gjelder masseovervåkning/bulkinnsamling som er omtalt i punkt 3.4.1.2, begrenset betydning for det foreliggende forslaget.

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. Når det gjelder data fra sosiale medier, vil dette være offentlig tilgjengelig data som brukere frivillig har lagt ut.

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.

Det er vanskelig å angi uttømmende hva som kan anses som åpent tilgjengelig informasjon. I etterretningstjenesteloven § 6-2 er det inntatt en negativ avgrensning, ved at det er angitt at informasjon ikke er åpent tilgjengelig dersom *«tilgang til informasjonen krever aktiv fordekt opptreden eller forsering av passord eller andre lignende beskyttelsesmekanismer»*. Etter departementets vurdering bør det inntas en lignende avgrensning i politiregisterloven, se forslag til lovendringer i punkt 7.2 nedenfor.

Lagring av åpent tilgjengelig informasjon vil i utgangspunktet kunne medføre brudd på regler om opphavsrett i åndsverksloven. Det følger imidlertid av åndsverksloven § 33 annet ledd at loven ikke er til hinder for at verk brukes i forbindelse med politiets kriminalitetsbekjempelse mv. Departementet legger derfor til grunn at åndsverksloven ikke legger noen begrensninger på PSTs muligheter til å lagre åpent tilgjengelig informasjon, slik det er foreslått i dette høringsnotatet.

5.2.4 Særskilt hjemmel for å behandle åpent tilgjengelig informasjon til etterretningsformål

Politiregisterloven har ikke noen eksplisitt hjemmel for å behandle opplysninger fra åpent tilgjengelige kilder. Dette er heller ikke nødvendig. Lovens system er at alle opplysninger, uavhengig av hvor de er hentet fra, må tilfredsstille kravene til formålsbestemthet, nødvendighet og relevans. Med den foreslåtte tydeliggjøringen av PSTs etterretningsoppdrag, jf. punkt 5.1, og den foreslåtte endringen i politiregisterloven § 64 tredje ledd nytt nr. 6, vil også PST kunne behandle åpent tilgjengelig informasjon til dette formålet, dersom vilkårene for øvrig er oppfylt.

Begrunnelsen for forslaget om en egen hjemmel for behandling av denne typen informasjon er at PST skal kunne oppfylle sitt etterretningsoppdrag og derfor må kunne lagre, systematisere og analysere et svært bredt spekter av informasjon, *selv om den enkelte opplysning ikke er nødvendig for dette formålet*. Forslaget åpner med andre ord for masseinnsamling av åpent tilgjengelig informasjon, uten en

vurdering av om den enkelte opplysning er av betydning for PSTs oppgaver. Som nevnt i punkt 5.2.1 er politiregisterloven tuftet på at kravene er knyttet til den enkelte opplysningen. Siden forslaget fraviker fra de alminnelige reglene om behandling av opplysninger, er det nødvendig å etablere en særskilt hjemmel for behandlingen. Departementet foreslår derfor en ny § 65 a i politiregisterloven som regulerer alle sider ved denne behandlingen, inkludert en forskriftshjemmel som oppstiller et krav til nærmere regulering i forskrift.

Departementet har vurdert om adgangen til å behandle offentlig tilgjengelig informasjon bør begrenses, for eksempel basert på konkrete informasjonsbehov eller lignende. En slik avgrensning er imidlertid vanskelig å gjennomføre i praksis. For å kartlegge utviklingen i trusselbildet, nylig oppståtte trusler eller nye trender, som på sikt kan få betydning for trusselbildet, er det nødvendig å kunne gå bredt ut. Ved en slik kartlegging vil man ikke vite sikkert hvor man finner informasjon som kan være av betydning. Det man ikke kjenner til, vet man heller ikke hvor man skal lete etter. Det vil derfor ikke være mulig å etablere egnede og tilstrekkelig presise avgrensingskriterier i regelverket for hvilke opplysninger som kan lastes ned.

I praksis vil PST selv kunne velge å avgrense innhentingen til noen kilder dersom disse anses å være av særlig stor interesse for etterretningsformålet, for eksempel der man har behov for å følge aktiviteten i såkalte «chan-fora» over tid for å kartlegge omfanget av ekstremistiske ytringer. Departementet mener imidlertid at det ikke bør oppstilles begrensninger i hva som *kan* hentes inn i regelverket, så lenge det er snakk om åpent tilgjengelig informasjon. En lovfestet begrensning i informasjonstilfanget vil medføre en risiko for at PST går glipp av viktig informasjon for etterretningsoppdraget, og vil dermed kunne ha som konsekvens at formålet med forslaget ikke oppnås.

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. Et eksempel er åpent tilgjengelige databaser fra Russland, som må lastes ned før man kan nyttiggjøre seg innholdet. Som eksempel fant en norsk avis flere russiske GRU-offiserer i Norge basert på et enkelt søk i et nedlastet russisk adresseregister. Journalistnettverket Bellingcat har brukt de russiske basene mye i undersøkende journalistikk. Etter departementets syn bør politiregisterloven legge til rette for at slik bruk av åpne kilder også er mulig for PST, der formålet er bekjempelse av alvorlig kriminalitet og ivaretakelse av nasjonal sikkerhet.

I lys av at forslaget åpner for behandling av svært store mengder åpent tilgjengelig informasjon, vil det kunne være nødvendig at behandlingen skjer helt eller delvis ved hjelp av automatiserte metoder for å kunne si noe om utvikling eller trender over tid. Forslaget her legger ikke føringer på *hvordan* opplysningene skal behandles for å ivareta etterretningsformålet. Departementet foreslår imidlertid av pedagogiske hensyn å innta i forskriften § 21-8 at behandling for etterretningsformål *kan* skje ved bruk av automatiserte analyseverktøy. Dette utelukker ikke at behandlingen kan skje med andre metoder. Eventuelle automatiserte analyseverktøy må innrettes slik at disse brukes til *etterretningsformål*, det vil si for å kartlegge trender og utviklingstrekk innenfor PSTs ansvarsområde, og i denne forbindelse utarbeide analyser og

etterretningsvurderinger. Bruk av automatiserte analyseverktøy kan dermed ikke skje med det formål å kartlegge enkeltindividers aktivitet på nett.

Departementet finner avslutningsvis grunn til å understreke at forslaget til ny § 65 a ikke medfører noen begrensninger for PSTs gjeldende adgang til å innhente og behandle åpent tilgjengelig informasjon. Som nevnt innledningsvis kan slike opplysninger behandles dersom de alminnelige kravene til behandlingen er oppfylt. Forslaget til ny § 65 a har heller ingen innvirkning på behandling av opplysninger etter § 65, hvoretter opplysninger kan behandles i fire måneder uten at kravene til formålsbestemthet, nødvendighet og relevans er oppfylt. Slike opplysninger kan også komme fra åpne kilder. Hovedforskjellen er at § 65 er ment å regulere enkeltstående opplysninger, mens forslaget til ny § 65 a åpner for masseinnsamling og behandling av åpent tilgjengelig informasjon.

5.2.5 Unntak fra kravene i § 6 om opplysningenes kvalitet og unntak fra § 7 om behandling av særlige kategorier av personopplysninger

Som nevnt i punkt 5.2.1 innebærer adgangen til å laste ned store mengder åpent tilgjengelig informasjon noe nytt som ikke passer inn i politiregisterlovens alminnelige regler om behandling av opplysninger. Det er derfor nødvendig å gjøre unntak fra flere av bestemmelsene i lovens kapittel 2, som blant annet stiller krav om formålsbestemthet, nødvendighet og krav til opplysningenes kvalitet.

De grunnleggende kravene om formålsbestemthet og nødvendighet vil etter departementets syn være oppfylt også for behandling etter den nye bestemmelsen. Formålet fremgår av forslaget til politiloven § 17 b fjerde ledd og politiregisterloven § 64 tredje ledd nytt nr. 6 om PSTs etterretningsvirksomhet. For etterretningsformålet er det etter departementets vurdering nødvendig at PST kan laste ned store mengder opplysninger fra internett selv om den enkelte opplysning i materialet isolert sett ikke vil være nødvendige for formålet. Nødvendighetskravet vil i denne sammenheng knytte seg til opplysningene *samlet sett*, og ikke til den enkelte opplysning. Departementet legger derfor til grunn at det ikke er behov for å gjøre unntak fra nødvendighetskravet.

Derimot er det nødvendig å gjøre unntak fra kravene i politiregisterloven § 6, herunder kravene til at opplysningene som behandles skal være relevante og korrekte. For enkeltstående opplysninger er det ofte vanskelig å trekke grensen mellom nødvendighetskravet og relevanskravet. Forskjellen mellom de to vilkårene kommer imidlertid klarere frem når nødvendighetskravet defineres så vidt som i forslaget. I særmerknaden til § 6 første ledd nr. 1 i Ot.prp. nr. 108 (2008-2009) på side 296 fremgår det at *«[h]ensikten med relevanskravet er å forhindre at det behandles flere opplysninger enn det er behov for».* Relevanskravet kommer dermed først og fremst til anvendelse der det registreres flere opplysninger, som isolert sett alle er nødvendige for formålet, men hvor det er tilstrekkelig å registrere bare en av dem for å oppnå formålet. Siden dette vil være situasjonen ved ubegrenset nedlasting av opplysninger fra åpne kilder, er det nødvendig å gjøre unntak fra relevanskravet.

I tillegg må det gjøres unntak fra kravet i politiregisterloven § 6 første ledd nr. 2, hvoretter opplysninger skal være korrekte og oppdaterte. Når informasjon publiseres på internett vil PST ikke ha noen mulighet til å vurdere om den enkelte opplysning faktisk er korrekt. Opplysningene vil kunne anses korrekte i den forstand at de fremkommer på den måten de har blitt publisert, uavhengig av om

de reelt sett stemmer. Et slikt unntak er for øvrig allerede nedfelt i politiregisterloven, ved at det følger av § 6 fjerde ledd at kravet om korrekthet i nærmere bestemte tilfeller er oppfylt når opplysningen er gjengitt slik kilden ga dem.

Utover dette er det behov for å gjøre unntak fra § 7, som gir anvisning på at behandling av særlige kategorier av opplysninger 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. Siden det ikke vil være mulig å filtrere ut slike opplysninger, kan § 7 ikke gjelde for denne typen behandling.

5.2.6 Begrensninger for behandlingen av opplysningene – særlig om sperring

Selv om departementet mener at PSTs samfunnsoppdrag tilsier at det åpnes for ubegrenset lagring av offentlig tilgjengelig informasjon, må de personvernmessige betenkelighetene ved ordningen kompenseres så langt det lar seg gjøre, herunder gjennom etablering av tilstrekkelige sikkerhetsmekanismer for å unngå misbruk.

I lys av den alminnelige proporsjonalitetsvurderingen som må foretas under EMK artikkel 8 nr. 2, må behovet for slike mekanismer ses i sammenheng med inngrepets alvor. Det at forslaget går ut på masseinnsamling av informasjon uten noen form for vurdering på individnivå, kan tilsi at inngrepet i utgangspunktet er begrenset. Videre må det ses hen til at innhentingen gjelder opplysninger som er offentlig tilgjengelige og ikke forutsetter bruk av tvangsmidler eller skjulte metoder.

Sett i lys av at inngrepet anses mindre alvorlig enn andre former for overvåking, mener departementet at særskilte regler om lagring av opplysningene, begrensinger i bruken og etterfølgende kontroll, sett i sammenheng med de alminnelige reglene om informasjonssikkerhet, internkontroll og sporing, vil ivareta de nødvendige kravene til sikkerhetsmekanismer.

Den nye ordningen vil medføre at PST kan behandle opplysninger om en stor andel av befolkningen, uten at opplysningene er systematisk innhentet på individnivå. Dette tilsier at man må begrense følgene for den enkelte i størst mulig grad. Departementet foreslår derfor at opplysningene i sin helhet skal s*perres*. At en opplysning er sperret innebærer en rekke konsekvenser som skiller seg markant fra de generelle reglene i politiregisterloven om behandling av opplysninger. Departementet finner derfor grunn til å gjøre nærmere rede for politiregisterlovgivningens regler om sperring.

Etter politiregisterloven § 2 nr. 10 innebærer sperring *«markering av lagrede opplysninger i den hensikt å begrense den fremtidige behandlingen av disse opplysningene»*. Sperrede opplysninger kan bare brukes til de formål som gjorde at opplysningen ikke ble slettet, jf. § 52. Dette innebærer at det må angis særskilt hvilke formål de sperrede opplysningene kan brukes til. Videre følger det av politiregisterforskriften § 15-2 annet ledd at opplysninger som er sperret skal holdes atskilt. De vil derfor ikke behandles sammen med andre opplysninger som behandles av PST. Tilgang til opplysninger som er sperret skal begrenses til så få personer som mulig, og bare gis til personer som har fått særskilt bemyndigelse.

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. Dette fremgår ikke eksplisitt av politiregisterloven, men er en konsekvens av at opplysningen er sperret. Som eksempel kan nevnes politiregisterloven § 41 om uttømmende politiattester, hvoretter straffer mv. som er «registrert» i reaksjonsregisteret skal anmerkes på slike attester. I merknadene til bestemmelsen i Ot.prp. nr. 108 (2008-2009) på side 314 fremgår det at *«[n]år bestemmelsen angir at det kun er opplysninger som er registrert i reaksjonsregisteret som skal anmerkes, så er dette for å markere at sperrede opplysninger ikke skal tas med»*.

Sperring er også etablert for registeret for Nasjonalt tverretatlig analyse- og etterretningssenter ved ØKOKRIM (NTAES) for å sikre at opplysningene bare kan brukes av medarbeidere ved senteret for formålene med registeret, jf. forskriften § 59-11. Også for overskuddsinformasjon fra kommunikasjonskontroll er det etablert en regel om sperring, jf. politiregisterloven § 50 tredje ledd:

«Opplysninger innhentet ved kommunikasjonskontroll som ikke er brukt i saken, skal sperres når saken er avgjort ved rettskraftig dom eller endelig henleggelsesbeslutning. Sperrede opplysninger kan benyttes ved begjæring om gjenåpning, ved gjenopptakelse av etterforskning, eller for å ivareta siktedes legitime interesser.»

Opplysninger som er sperret etter denne bestemmelsen vil kunne være lagret i svært lang tid.

Overført til PSTs virksomhet innebærer forslaget om at opplysningene skal sperres at PST ikke kan søke i disse opplysningene i forbindelse med for eksempel sikkerhetsklareringer, henvendelser fra andre organer eller andre løpende oppgaver. Opplysningene vil heller ikke kunne utleveres til andre.

Dersom opplysningene skal kunne brukes til andre formål enn etterretningsvirksomhet, må dette reguleres særskilt.

Departementet mener de sperrede opplysningene også bør kunne brukes i de tilfellene der det er åpnet etterforsking eller i forbindelse med en forebyggende sak, men at det ellers ikke bør åpnes for bruk til andre formål. Dersom det i de sperrede opplysningene finnes informasjon om personer som PST allerede har i søkelyset, eksempelvis der det er opprettet forebyggende sak eller der det pågår en etterforsking, eller om personer som utgjør en reell trussel, bør PST kunne behandle denne informasjonen.

Forebyggende sak opprettes når det er grunn til å undersøke om noen forbereder et straffbart forhold som PST har til oppgave å forebygge, jf. politiregisterloven § 64 tredje ledd nr. 1 og forskriften § 21-5. Formålet med den forebyggende saken er å skaffe til veie nødvendige opplysninger og iverksette nødvendige tiltak for å forebygge straffbare handlinger innenfor PSTs oppgaver etter politiloven § 17 b. Når PST først har gått til det skritt å opprette en forebyggende sak, vil man søke 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 de sperrede materiale gjelder også 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.

Det er gitt regler i forskriften § 21-5 om hvem som skal godkjenne opprettelse av forebyggende sak. Det vil dermed være en kontroll av om opplysningene kvalifiserer til opprettelse av forebyggende sak. Gjør de ikke det, vil de heller ikke kunne brukes. Opplysningene kan dermed ikke brukes til forebygging i alminnelighet. Dette innebærer eksempelvis at PST ikke vil kunne bruke det sperrede materialet til kartlegge nettaktiviteten til personer som på sikt kanskje kan utgjøre en trussel, men der vilkårene for å opprette forebyggende sak ikke er oppfylt.

Når det gjelder bruk til etterforsking, foreslår departementet ikke ytterligere begrensninger enn at det må dreie seg om etterforsking av lovbrudd som nevnt i politiloven § 17 b. Opplysningene vil også kunne brukes til å åpne etterforsking. Etterforsking 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, jf. straffeprosessloven § 224. 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, mener departementet at PST må kunne søke i de sperrede opplysningene for å klarlegge om det finnes opplysninger der av betydning for straffesaken. I motsatt fall vil man kunne risikere at avgjørende bevismateriale ikke avdekkes, og at skyldige personer går fri.

Både forebygging og etterforsking av de straffbare handlinger som er nevnt i politiloven § 17 b har nær sammenheng med PSTs etterretningsvirksomhet. Departementet anser derfor ikke slik bruk for å være en formålsutglidning. PST har allerede i dag mulighet til å benytte åpent tilgjengelig informasjon i forbindelse med forebygging og etterforsking. Det er også verdt å minne om at PST i etterforskingssporet, på lik linje med det øvrige politiet, kan benytte seg av straffeprosesslovens tvangsmidler, herunder kommunikasjonskontroll og dataavlesing, for å innhente relevant informasjon. I motsetning til det øvrige politiet, kan PST også for flere typer handlinger benytte seg av tvangsmidler også i det forebyggende sporet, jf. politiloven § 17 d. Bruk av skjulte tvangsmidler 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, i motsetning til det mer overordnede trusselbildet som er av interesse ved behandling til etterretningsformål. En slik bruk vil kunne være mer inngripende for personene det søkes etter. Departementet har derfor vurdert om det bør oppstilles ytterligere vilkår for bruk av de sperrede opplysningene for disse formålene, herunder om det bør stilles krav om en forutgående kontroll. Departementet er ikke kjent med eksempler på ordninger hvor det oppstilles krav om domstolskontroll ved bruk av opplysninger det allerede er lovlig grunnlag for å behandle. Departementet kan heller ikke se at et slikt krav kan utledes av EMDs praksis. Selv om EMD i forbindelse med bulkinnsamling av grensekryssende informasjon har lagt til grunn at inngrepet i individets rettigheter etter artikkel 8 tiltar underveis i prosessen, jf. omtalen i punkt 3.4.1.2 ovenfor, er ikke dette

direkte overførbart til behandling av opplysninger etter forslaget her, ettersom dommene gjelder en annen og mer inngripende form for masseinnhenting. Departementet legger derfor til grunn at det ikke bør stilles krav om forutgående kontroll for søk til disse formålene.

5.2.7 Saksbehandling og kontroll

Som nevnt i punkt 5.2.6 følger det allerede av politiregisterforskriften § 15-2 at opplysninger som sperres skal holdes atskilt, at tilgang kan gis til et begrenset antall personer og at disse må ha særskilt bemyndigelse. Etter departementets vurdering bør dette likevel også presiseres særskilt i tilknytning til opplysningene dette forslaget gjelder, jf. forskriftsforslaget § 21-8. Departementet finner imidlertid ikke grunn til å innta et krav om at tilgangen skal begrenses til så få personer som mulig. Ved at det stilles krav om bemyndigelse, vil det uansett foretas en vurdering av behovet for tilgang. Det forutsettes at slik tilgang ikke gis til flere personer enn nødvendig.

For å kunne kontrollere at søkene er lovlige, foreslås det en regel i § 21-8 om at all bruk av opplysninger skal registreres og kunne spores. Registreringer skal gjennomgås regelmessig med det formål å avdekke eventuell uautorisert tilgang til opplysningene. Denne regelen følger allerede av forskriften § 40-13 om sikkerhetstiltak og sporbarhet. Siden det ikke fremkommer eksplisitt at reglene i kapittel 40 gjelder så langt de passer for PST, bør denne regelen etter departementets syn også fremgå av forskriftsbestemmelsen om behandling av opplysninger i medhold av § 65 a.

Ut over dette foreslår ikke departementet særlige regler om behandlingen av de sperrede opplysningene. 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 i den nye bestemmelsen.

Lovens kapittel 4 med tilhørende forskriftsregler stiller en rekke krav om informasjonssikkerhet, internkontroll og krav til sporbarhet. Som nevnt vil sporbarhet være en viktig mekanisme for å sikre at lovens regler overholdes, og vil sikre at det kan føres tilstrekkelig kontroll. Etter politiregisterforskriften § 23-1 om informasjonssikkerhet er Sjef PST *«ansvarlig for at det til enhver tid er iverksatt tiltak for nødvendig sikring av konfidensialitet, integritet og tilgjengelighet for opplysninger som behandles i PST, i samsvar med bestemmelsene i sikkerhetsloven med tilhørende forskrift og beskyttelsesinstruksen»*. Heller ikke krav til informasjonssikkerhet er det derfor nødvendig å regulere særskilt. Etter § 23-2 gjelder bestemmelsene i forskriften kapittel 39 om internkontroll tilsvarende for PST så langt de passer. Det følger av § 39-3 at den behandlingsansvarlige blant annet skal ha rutiner for bruk av opplysninger som er sperret. Dette vil også gjelde for behandling etter den nye bestemmelsen, og det anses derfor ikke nødvendig å regulere nærmere krav til rutiner i forskriftsbestemmelsen.

EOS-utvalget er tilsynsmyndighet for PST, og fører kontroll både av eget tiltak og på begjæring fra personer som antas å være registrert, jf. politiregisterloven § 68. EOS-utvalgets kontroll vil være en viktig sikkerhetsmekanisme. Kontroll med hvem som har tilgang til de sperrede opplysningene vil være en naturlig del av EOS-utvalgets kontroll med tjenesten. Ved at det stilles krav om bemyndigelse for tilgang til opplysningene, vil EOS-utvalget kunne kontrollere at slik tilgang kun

gis i nødvendig utstrekning. EOS-utvalget vil også kunne føre kontroll med søk i opplysningene, og at disse kun skjer for de formål loven åpner for.

Etter politiregisterloven § 66 er det ikke innsynsrett i opplysninger som behandles av PST. Begrunnelsen for dette er at en eventuell innsynsordning for opplysninger i PST ikke ville medføre en reell innsynsrett, idet unntakene fra innsyn på grunn av hensynet til blant annet rikets sikkerhet, kildevern og metodebruk ville komme til anvendelse i nærmest samtlige tilfeller, jf. Ot.prp. nr. 108 (2008-2009) punkt 17.4.3. Denne begrunnelsen gjør seg ikke fullt ut gjeldende for opplysninger som behandles etter forslaget her, ettersom det er snakk om åpent tilgjengelig informasjon, der innhentingen ikke er rettet mot spesifikke personer. Som nevnt i punkt 5.2.4 vil det imidlertid kunne være at PST avgrenser hvilke kilder de innhenter åpent tilgjengelig informasjon fra, selv om ikke regelverket oppstiller slike begrensninger. Å åpne for innsyn vil kunne innebære en risiko for at det avsløres hvilke områder på nettet PST velger å laste ned informasjon fra, slik at trusselaktører tilpasser sin aktivitet ut fra dette. Dette ville være meget uheldig, og vil kunne medføre at effekten av det nye virkemiddelet blir skadelidende.

I tillegg vil merverdien av innsyn være begrenset, all den tid den enkelte fritt kan søke opp informasjon som er publisert på internett om en selv. Videre er et viktig hensyn bak innsynsreglene å føre kontroll med opplysningens riktighet, noe som ikke er aktuelt her. Den potensielle administrative belastningen ved å pålegge PST å behandle slike innsynsbegjæringer står dermed etter departementets syn ikke i forhold til nytteverdien som tradisjonelt forbindes med innsynsretten.

Etter departementets syn bør det derfor ikke åpnes for innsyn i opplysninger som er lastet ned etter den nye bestemmelsen, slik at politiregisterloven § 66 vil gjelde på vanlig måte.

5.2.8 Sletting

For å kunne følge med på utvikling og endringer i trusselbildet vil det være behov for å lagre opplysninger over tid. Ved langtidslagring vil det være mulig å analysere utviklingen på området som følges, og se hvordan denne endrer seg i et lengre perspektiv. 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 mener at det er viktig at opplysningene ikke slettes så tidlig at formålet med forslaget ikke oppnås. Samtidig vil for lang lagringstid kunne innebære at inngrepet etter hvert anses uforholdsmessig. Etter departementets syn bør det derfor settes en ytre grense for hvor lenge de sperrede opplysningene kan lagres.

Politiregisterforskriften § 22-3 om sletting oppstiller ikke konkrete slettefrister for opplysninger som behandles av PST. I stedet er det etablert frister for når opplysninger skal gjennomgås. Eksempelvis skal arbeidsregistreringer som ikke er tilført nye opplysninger etter 5 år gjennomgås, og opplysningene skal slettes når de ikke lenger er nødvendige for formålet. En plikt til jevnlig vurdering vil ikke være egnet for opplysningene som behandles etter den nye bestemmelsen. En slik gjennomgang vil være svært ressurskrevende, samtidig som man nettopp ikke vil

vite om de enkelte opplysningene er nødvendig. Departementet har derfor i stedet sett hen til reglene i etterretningstjenesteloven § 9-8 om sletting av rådata i bulk, jf. omtalen i punkt 3.3, og foreslår at opplysningene skal slettes senest etter 15 år. Departementet ser at det også er hensyn som taler for en kortere slettefrist enn 15 år. Det bes derfor særlig om høringsinstansenes syn på slettefristen.

Det understrekes at den foreslåtte fristen på 15 år er en lengstefrist. PST vil derfor måtte slette opplysningene tidligere dersom tjenesten blir klar over at eksempelvis et nedlastet datasett ikke inneholder opplysninger av etterretningsmessig verdi, eller det av andre grunner ikke lenger er nødvendig for etterretningsformål. Dersom opplysningene brukes i forebyggende sak eller i etterforsking, jf. punkt 5.2.6 over, vil de kunne behandles videre etter de alminnelige reglene i henholdsvis forskriften del 6 og del 7.

Etterretningstjenesteloven § 9-8 åpner for å lagre informasjonen ut over 15 år dersom vesentlige hensyn tilsier at sletting utsettes. Departementets foreløpige vurdering er at det ikke er behov for en tilsvarende mulighet for forlenget lagring av opplysninger som behandles etter den nye bestemmelsen.

6 Økonomiske og administrative konsekvenser

Forslaget om å tydeliggjøre PSTs etterretningsoppdrag i politiloven vil ikke ha økonomiske eller administrative konsekvenser av betydning. PST vil måtte prioritere mellom ulike oppgaver innenfor de til enhver tid gjeldende budsjettrammer.

Forslaget om å gi hjemler for behandling av åpent tilgjengelig informasjon til etterretningsformål vil medføre behov for modernisering eller utvikling av IKT-systemer som kan håndtere mengden informasjon og analysere den. Det må også sikres nødvendig lagringskapasitet. I tillegg vil det kreves kompetanseheving i form av opplæring og/eller rekruttering, herunder styrking av internkontrollen i tjenesten. Hjemlene vil kunne tas i bruk i begrenset omfang, men med god effekt for tjenestens oppgaveløsning, med mindre teknologiske investeringer. PST anslår at dette vil koste om lag 2 millioner kroner, som vil kunne dekkes innenfor gjeldende budsjettrammer. Anslaget er usikkert.

For å kunne utnytte mulighetsrommet som lovendringene gir fullt ut, vil det imidlertid være behov for ytterligere investeringer for å sikre et system som har kapasitet til å håndtere mengden data, og som har mekanismer for tilgangskontroll, notoritet over bruk og kontroll av bruken. Videre er det behov for gode analyseverktøy for å nyttiggjøre seg opplysningene. Kostnadene ved dette må utredes nærmere. Forslag fra regjeringen som krever budsjettendringer vil bli fremmet for Stortinget i forbindelse med de årlige budsjettfremleggene.

Det kan ikke utelukkes at forslaget vil medføre at EOS-utvalget vil motta flere begjæringer om kontroll. I tillegg vil det være naturlig at utvalget regelmessig kontrollerer PSTs bruk av sperrede opplysninger, herunder også hvem som har tilgang til de sperrede opplysningene. Dette skiller seg imidlertid i begrenset grad fra den kontrollen utvalget allerede gjennomfører for PSTs del, og departementet antar at dette vil kunne dekkes innenfor utvalgets tildelte budsjettrammer.

7 Forslag til lov- og forskriftsendringer

7.1 Endringer i politiloven

§ 17 a kan lyde:

§ 17 a *Politiets sikkerhetstjeneste*

De gjøremål som er nevnt i § 17 b utføres av et eget politiorgan (Politiets sikkerhetstjeneste). *Politiets sikkerhetstjeneste er i tillegg til et politiorgan også Norges nasjonale innenlands etterretningstjeneste.* Tjenesten ledes av en sentral enhet.

§ 17 b nytt fjerde ledd kan lyde:

PST skal drive etterretningsvirksomhet i tilknytning til oppgaver som nevnt i første ledd og § 17 c nr. 1, herunder kartlegge trender og utviklingstrekk som har tilknytning til dette formålet, og i denne forbindelse utarbeide analyser og etterretningsvurderinger.

7.2 Endringer i politiregisterloven

§ 64 tredje ledd nytt nr. 6 kan lyde:

Utenfor den enkelte straffesak kan opplysninger bare behandles av Politiets sikkerhetstjeneste der det

[…]

6. *er nødvendig for etterretningsvirksomheten, jf. politiloven § 17 b fjerde ledd.*

Ny § 65 a kan lyde:

§ 65 a *Behandling av åpent tilgjengelig informasjon til etterretningsformål*

Politiets sikkerhetstjeneste kan behandle åpent tilgjengelig informasjon for etterretningsformål, jf. § 64 tredje ledd nr. 6, uten at bestemmelsene i §§ 6 og 7 kommer til anvendelse. Informasjon er ikke åpent tilgjengelig dersom tilgang krever forsering av passord eller lignende beskyttelsesmekanismer.

Opplysninger som behandles etter denne bestemmelsen skal sperres, og kan bare brukes til følgende formål:

1. *PSTs etterretningsvirksomhet, jf. politiloven § 17 b fjerde ledd*
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 15 år.

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

7.3 Endringer i politiregisterforskriften

Ny § 21-8 kan lyde:

§ 21-8 *Særlig om behandling av åpent tilgjengelig informasjon etter politiregisterloven § 65 a*

Opplysninger som behandles etter politiregisterloven § 65 a skal holdes atskilt. Tilgang til opplysningene skal bare gis til personer som har fått særskilt bemyndigelse.

Behandling av opplysningene for etterretningsformål, jf. § 65 a tredje ledd nr. 1, kan skje ved bruk av automatiserte analyseverktøy.

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.