



UiT Norges arktiske universitet

Det juridiske fakultet

PSTs adgang til innhenting, lagring og behandling av åpent tilgjengelig informasjon

En vurdering i lys av EMK artikkel 8

Sofie Salomonsen Klette

Masteroppgave i rettsvitenskap, JUR-3902, vår 2022

Innholdsfortegnelse

1	Innledning.....	1
1.1	Problemstilling og aktualitet	1
1.2	Kort om PST og forslaget.....	3
1.3	Metode.....	5
1.3.1	Utgangspunkter	5
1.3.2	EMK-rettslig metode.....	5
1.4	Avgrensninger og fremstillingen videre.....	7
2	Generelt om retten til privatliv	9
3	Inngrep	11
3.1	Introduksjon	11
3.2	Arten av inngrepet, hvordan det rammer og hvor tyngende det er overfor den som rammes	11
3.2.1	Rettslige utgangspunkter	11
3.2.2	Generelt om inngrepsgrad vedrørende «åpent tilgjengelig informasjon»	13
3.2.3	Innhenting og den innledende oppbevaringen av data	16
3.2.4	Behandling av det innhentede materialet	16
3.2.5	Påfølgende oppbevaring av data og deling med andre.....	19
3.3	Konklusjon	20
4	Legitimt formål	21
4.1	Utgangspunkter	21
4.2	Hvilket legitime formål forfølges ved PSTs innhenting, lagring og behandling av åpent tilgjengelig informasjon?.....	21
5	Rettmessighet	23
5.1	Introduksjon	23
5.2	Rettmessighetsvurderingen i saker fra EMD om bulkinnsamling	23
5.3	Rettsikkerhetsmekanismer i EMDs praksis	24

5.4	Er PSTs adgang til innhenting, lagring og behandling av åpent tilgjengelig informasjon et rettmessig inngrep i EMK artikkel 8?	27
5.4.1	Grunnlaget for at bulkinnhenting kan tillates	27
5.4.2	Hvilke omstendigheter som kan medføre innhenting av enkeltpersoners kommunikasjon	28
5.4.3	Hvilke prosedyrer som gjelder for å gi autorisasjon til innhenting	30
5.4.4	Hvilke prosedyrer som gjelder for seleksjon, analyse og bruk av innhentede data	31
5.4.5	Hvilke forholdsregler som må tas dersom innhentede data deles med andre ..	37
5.4.6	Tidsbegrensninger for innhenting, lagring av innhentet data og omstendighetene som gjør at innhentet data må slettes	39
5.4.7	Hvilke prosedyrer som gjelder for uavhengig tilsyn og kontroll, og deres kompetanse til å adressere manglende etterlevelse	41
5.4.8	Hvilke prosedyrer som gjelder for uavhengig etterhåndskontroll, og hvilken kompetanse kontrollorganet har til å adressere manglende etterlevelse	43
5.4.9	Den samlede vurderingen og konklusjon	45
6	Avsluttende refleksjoner	48
	Referanseliste	49

1 Innledning

1.1 Problemstilling og aktualitet

Avhandlingens tema er forslaget om Politiets sikkerhetstjenestes (heretter PST) adgang til innhenting, lagring og behandling av åpent tilgjengelig informasjon¹ og retten til privatliv etter Den europeiske menneskerettighetskonvensjonen² (heretter EMK) artikkel 8.

Høringsnotatet med forslaget om politiregisterloven³ ny § 65 a⁴ vedrørende PSTs adgang til innhenting, lagring og behandling av åpent tilgjengelig informasjon ble publisert av Justis- og beredskapsdepartementet (heretter departementet) 7. oktober 2021. Høringsfristen gikk ut 7. januar 2022. Forslaget innebærer at PST kan innhente, lagre og behandle åpent tilgjengelig informasjon til etterretningsformål. Videre skal opplysningene sperres, og slettes senest etter 15 år.⁵ Forslaget vil medføre en utvidet bruk av åpent tilgjengelig informasjon for PST. Herunder at PST kan behandle store mengder informasjon som kan inneholde opplysninger om enkeltpersoners privatliv. Etter publiseringen har forslaget blitt kritisert i høringsuttalelser, sosiale medier og det juridiske miljøet. Datatilsynet uttaler at «Forslaget innebærer at PST går fra å være en politimyndighet som driver forebygging og etterforskning av konkret angitte straffbare handlinger, til å bli en tjeneste som driver etterretning mot norske borgere»⁶ og i tilsynets høringsuttalelse omtales det som en «ubegrenset nedlastning av opplysninger fra åpne kilder» for PST.⁷

Det er foreslått at PST kan anvende teknologiske verktøy til innhenting, lagring og behandling av informasjon fra åpne kilder, herunder helt eller delvis med automatiserte analyseverktøy.⁸ Dagens samfunn er i stadig teknologisk utvikling gjennom økt fokus på digitalisering. Det kan påstås at den teknologiske bølgen siden tusenårsskiftet har handlet om informasjon. Informasjonsteknologi er teknologi der informasjon bearbeides, lagres og

¹ Høring om endringer i politiloven og politiregisterloven mv. PSTs etterretningsoppdrag og behandling av åpent tilgjengelig informasjon, 7. oktober 2021 (heretter høringsnotatet eller forslaget).

² Convention for the Protection of Human Rights and Fundamental Freedoms, Roma, 4. november 1950 (Den europeiske menneskerettighetskonvensjonen – EMK).

³ Lov 28. mai 2010 nr. 16 om behandling av opplysninger i politiet og påtalemyndigheten (politiregisterloven)

⁴ Høringsnotatet punkt 7.2.

⁵ Høringsnotatet punkt 1.

⁶ Datatilsynets hjemmesider: <https://www.datatilsynet.no/aktuelt/aktuelle-nyheter-2022/horing-om-pst-og-behandling-av-اپent-tilgjengelig-informasjon/> (lest 27.01.2022).

⁷ Se Datatilsynets høringsuttalelse 05.01.2022 til Justis- og beredskapsdepartementet side 1.

⁸ Høringsnotatet punkt 5.2.4 spalte 6, punkt 6, og punkt 7.3 forslag til politiregisterforskriften ny § 21-8 annet ledd.

formidles som tekst, lyd eller bilder i digital form.⁹ Digitaliseringen i det offentlige handler om å forenkle, forbedre og effektivisere teknologi.¹⁰ Ettersom informasjon kan deles og kopieres mellom maskiner og databaser, kan myndighetene arbeide raskere enn ved tidligere analoge metoder. Eksempelvis kan PST innhente informasjon fra flere kilder og behandle denne informasjonen langt mer effektivt enn tidligere. Følgelig har teknologiutviklingen medført at staten kan ta i bruk mer effektive midler for å løse sine samfunnsoppdrag. Teknologibølgen og den stadige moderniseringen av samfunnet utgjør samtidig en utfordring for befolkningens personvern. I dagens samfunn er det flere eksempler på hackerangrep hvor personopplysninger havner på avveie og at informasjon om borgerne brukes for å manipulere demokratiske prosesser.¹¹ På bakgrunn av dette kan det hevdes at borgernes privatliv aldri har vært under større press enn i dag.

Kritikken til forslaget om politiregisterloven § 65 a i høringsnotatet har blant annet knyttet seg til vurderingen av retten til privatliv, særlig i relasjon til EMK artikkel 8. Departementet legger til grunn at PSTs adgang til innhenting, lagring og behandling av åpent tilgjengelig informasjon er i tråd med EMK artikkel 8.¹² Advokatforeningen har i høringsuttalelsen fremholdt at departementets vurderinger på dette punktet fremstår som «overfladiske og dets konklusjoner som tynt begrunnet».¹³ I denne utstrekning er den ene hovedproblemstillingen i avhandlingen om forslaget til politiregisterloven ny § 65 a er i tråd med EMK artikkel 8.

En annen del av forslaget om politiregisterloven § 65 a som er kritisert, er departementets vurdering i høringsnotatet av EMK artikkel 8 og den tilhørende praksis fra Den europeiske menneskerettighetsdomstolen (heretter EMD). Særlig knyttes dette til departementets vurdering av de to avsagte avgjørelsene fra EMD om bulkinnsamling i 2021, henholdsvis *Centrum för rättvisa*¹⁴ og *Big Brother Watch*¹⁵. Norges institusjon for menneskerettigheter fremholder i høringsuttalelsen at «departementets analyse av EMDs rettspraksis om

⁹ Eirik Rossen, "IT" i Store norske leksikon, 6. november 2019, <https://snl.no/IT> (lest 10.03.2022).

¹⁰ Regjeringens hjemmesider: <https://www.regjeringen.no/no/tema/statlig-forvaltning/ikt-politikk/digitaliseringen-i-offentlig-sektor/id2340245/> (lest 23.02.2022).

¹¹ Se eksempelvis Tore Letvik og Tuva Bønke Grønning, «Hacking og datalekkasjer utgjør en stor trussel for personvernet», *Juristen*, 16. mars 2022 <https://juristen.no/nyheter/2022/02/—hacking-og-datalekkasjer-utgjør-en-stor-trussel-personvernet> (lest 05.04.2022).

¹² Høringsnotatet punkt 5.2.2.

¹³ Advokatforeningens høringsuttalelse 03.01.2022 til Justis- og beredskapsdepartementet punkt 3.1.

¹⁴ *Centrum för rättvisa mot Sverige* [GC] 2021, no. 35252/08 (heretter *Centrum för rättvisa*).

¹⁵ *Big Brother Watch og andre mot Storbritannia* [GC] 2021, nos. 58170/13, 62322/14 and 24960/15 (heretter *Big Brother Watch*).

masseovervåking og bulkinnsamling er mangelfull» og «etterlyser også i hvilken grad departementet mener rettspraksisen kan få overføringsverdi for forslaget, og en begrunnelse for dette.»¹⁶ EOS-utvalget har også påpekt dette i sin høringsuttalelse, hvorav det etterlyses «en nærmere vurdering av hvilken overføringsverdi dommene har til departementets forslag.»¹⁷ EMD har ikke direkte behandlet spørsmålet om myndighetenes adgang til innhenting, lagring og behandling av åpne kilder. Følgelig er den andre hovedproblemstillingen i avhandlingen hvordan PSTs adgang til innhenting, lagring og behandling av åpent tilgjengelig informasjon skal behandles etter EMK artikkel 8.

Til tross for at høringsnotatet har blitt møtt med mange høringsuttalelser, foreligger det ikke autoritative kilder som har vurdert om masseinnsamling av åpne kilder er i tråd med EMK artikkel 8. Dermed vil dette undersøkes nærmere i denne avhandlingen.

1.2 Kort om PST og forslaget

PST er «et eget politiorgan», jf. politiloven¹⁸ § 17 a første punktum, og er opprettet i medhold av politiloven § 16 tredje ledd nr. 1. PST er direkte underlagt Justisdepartementet, jf. Instruks for Politiets sikkerhetstjeneste¹⁹ § 2 første ledd. Etter politiloven § 17 a siste punktum ledes PST av en sentral enhet. PST skal forebygge og etterforske alvorlig kriminalitet mot nasjonens sikkerhet.²⁰ I høringsnotatet er det foreslått å innlemme i politiloven § 17 a annet punktum, at «Politiets sikkerhetstjeneste er i tillegg til et politiorgan også Norges nasjonale innenlands etterretningstjeneste».²¹ Dette er for å tydeliggjøre PSTs oppgaver og at det er en innlands etterretningstjeneste.²² EOS-utvalget er tilsynsorganet for PST ved behandling av informasjon, jf. politiregisterloven § 68 og EOS-kontrollloven²³ § 6 fjerde ledd punkt 1. EOS-utvalget er underlagt Stortinget²⁴ og i tillegg til PST fører det kontroll med Etterretningstjenesten, Nasjonal sikkerhetsmyndighet og Forsvarets sikkerhetsavdeling²⁵.

¹⁶ Norges institusjon for menneskerettigheters høringsuttalelse 07.01.2022 til Justis- og beredskapsdepartementet punkt 3.3.

¹⁷ EOS-utvalgets høringsuttalelse 17.12.2021 til Justis- og beredskapsdepartementet punkt 2.2.

¹⁸ Lov 4. august 1995 nr. 53 om politiet (politiloven).

¹⁹ Instruks 19. august 2005 nr. 920 for Politiets sikkerhetstjeneste.

²⁰ PSTs hjemmesider: <https://www.pst.no/alle-artikler/artikler/dette-gjor-vi/> (lest 15.03.2022).

²¹ Høringsnotatet punkt 7.1.

²² Høringsnotatet punkt 5.1.2.

²³ Lov 3. februar 1995 nr. 7 om kontroll med etterretnings-, overvåkings- og sikkerhetstjenestene (EOS-kontrollloven).

²⁴ Jf. EOS-kontrollloven § 1 første ledd.

²⁵ Jf. EOS-kontrollloven § 6 fjerde ledd.

PST har som formål å forebygge og etterforske nærmere angitte oppgaver, jf. politiloven § 17 b, og skal drive etterretningsvirksomhet, jf. eksempelvis § 17 c punkt 1 og høringsnotatet punkt 7.1. PST skal ved sitt forebyggende arbeid blant annet «innhente, bearbeide, analysere og utveksle informasjon i samsvar med fastsatte prioriteringer», jf. Instruks for Politiets sikkerhetstjeneste § 5 første ledd. Definisjon på «forebyggende sak» fremgår av Politiregisterforskriften²⁶ § 20-3 punkt 2, som «sak som opprettes når det er grunn til å undersøke om noen forbereder et straffbart forhold som PST har til oppgave å forebygge». Etterforskning og påtalemessige forhold for PST reguleres etter bestemmelsene i straffeprosessloven, påtaleinstruksen og bestemmelser fra overordnet påtalemyndighet, jf. Instruks for Politiets sikkerhetstjeneste § 2 annet ledd. Vedrørende etterretningsvirksomheten i PST skal det foretas trusselvurderinger og sikkerhetsrådgivning. Herunder skal PST utarbeide trusselvurderinger og gi råd om tiltak, jf. Instruksen § 6 første ledd.

PST har etter dagens regelverk adgang til å behandle informasjon fra åpne kilder ut ifra oppgavene som fremgår av politiloven. Så fremt det er i samsvar med politiregisterlovens regler. Forslaget om politiregisterloven § 65 a innebærer at PST skal ha en utvidet adgang til behandling av åpent tilgjengelig informasjon. Herunder at all informasjon fra åpne kilder kan behandles til rene etterretningsformål.²⁷ Politiregisterlovens regler i dag om behandling av opplysninger åpner ikke for å lagre, systematisere og analysere store mengder åpent tilgjengelig informasjon.²⁸ Dette er begrunnelsen for forslaget om politiregisterloven § 65 a.

Behandling av opplysninger er definert i politiregisterloven § 2 punkt 2 som «enhver elektronisk eller manuell bruk av opplysninger». For behandling av opplysninger i PST gjelder politiregisterloven, jf. politiregisterforskriften del 6 og Instruks for Politiets sikkerhetstjeneste § 19 første ledd første punktum. Politiregisterloven kapittel 11 inneholder særbestemmelser for PST og utfylles i politiregisterforskriften del 6. Formålet med PSTs behandling av opplysninger er at det skal bidra til beskyttelse av personvernet og forutberegnelighet for den enkelte, jf. politiregisterloven § 1. Loven inneholder krav til behandling av opplysninger i kapittel 2. Departementet har i høringsnotatet lagt til grunn at kravene til formålsbestemthet etter § 4 og nødvendighet etter § 5 er oppfylt ved ny § 65 a i

²⁶ Forskrift 20. september 2013 nr. 1097 om behandling av opplysninger i politiet og påtalemyndigheten (politiregisterforskriften).

²⁷ Høringsnotatet punkt 2.2.

²⁸ Høringsnotatet punkt 2.2.

politiregisterloven. I høringsnotatet foreslås det imidlertid unntak fra § 6 om krav til opplysningenes kvalitet og § 7 som stiller særskilte krav til behandling av særlige kategorier av personopplysninger.²⁹

1.3 Metode

1.3.1 Utgangspunkter

Avhandlingen er en rettsdogmatisk fremstilling. «Rettsdogmatikk» er en deskriptiv fremstilling av gjeldende rett hvor innholdet av gjeldende rettsregler skal klarlegges.³⁰ Oppgaven står i en særstilling ettersom forslaget om politiregisterloven § 65 a ikke har trådt i kraft og derav ikke er gjeldende rett. Avhandlingens vurdering kan innebære konklusjoner om at forslaget kan lovfestes i den form det er fremsatt i tråd med EMK artikkel 8, eller, dersom det konstateres strid, at forslaget ikke burde fremsettes slik det er foreslått. På denne måten vil fremstillingen også være preskriptiv.

Lovforslaget skal imidlertid vurderes opp imot gjeldende rett, herunder det tilhørende regelverket ved PSTs behandling av informasjon og EMK artikkel 8. Dermed skal det i avhandlingen foretas en rettsdogmatisk analyse av om forslaget til ny § 65 a i politiregisterloven sammenholdt med det tilhørende regelverket er i tråd med EMK artikkel 8. I avhandlingen skal forslaget om politiregisterloven § 65 a vurderes som om det var lovfestet i den form det er foreslått.

I fremstillingen skal EMK artikkel 8 analyseres. Dermed er det hensiktsmessig å gjøre rede for generelle metodiske særpreg ved EMK-retten, og metodiske utfordringer i avhandlingen.

1.3.2 EMK-rettslig metode

Gjennom menneskerettsloven³¹ ble EMK inkorporert i norsk rett med forrang foran annen lovgivning i 1999, jf. mrl. §§ 2 og 3.

EMD er opprettet i medhold av EMK artikkel 19. EMD har som oppgave å sikre at forpliktelsene til konvensjonen blir opprettholdt. EMD er den siste og autoritative fortolker av EMK, jf. EMK artikkel 32 nr. 1. Det er medlemsstatene som er pliktsubjekt for konvensjonen

²⁹ Høringsnotatet punkt 5.2.5.

³⁰ Jens Edvin A. Skoghøy, *Rettsdogmatikk*, Universitetsforlaget 2018, side 25.

³¹ Lov 21. mai 1999 nr. 30 om styrking av menneskerettighetenes stilling i norsk rett (menneskerettsloven – mrl.).

og som i første rekke skal anvende og respektere konvensjonen.³² Dette ansvaret følger av subsidiaritetsprinsippet som ved protokoll 15 ble inntatt i fortalet til EMK.³³

Subsidiaritetsprinsippet går ut på at EMD skal ha en subsidiær rolle og kun gripe inn dersom det er nødvendig.³⁴ EMD har vært intensiv i sin prøving når det gjelder masseinnsamling av data om borgerne og oppstilt forholdsvis klare vilkår.³⁵ Dette tilsier at EMD anser denne type aktivitet fra myndighetene som et alvorlig inngrep.

EMD har lagt til grunn at EMK skal tolkes i samsvar med Wien-konvensjonen om traktatretten³⁶ artikkel 31 til 33.³⁷ Ordlyden av konvensjonsteksten er utgangspunktet for tolkningen, og må tolkes sammen med dens kontekst, gjenstand og formål, jf. Wien-konvensjonen artikkel 31 nr. 1. EMD har utviklet egne tolkningsprinsipper i tillegg til de generelle tolkningsprinsippene som fremgår av Wien-konvensjonen. Det følger av EMDs praksis i avgjørelsen *Tyrer mot Storbritannia* at «[...] the Convention is a living instrument which, [...] must be interpreted in the light of present-day conditions.»³⁸ Ettersom konvensjonsteksten er vagt formulert, skal gjelde over tid, og favne over flere land med ulike rettstradisjoner, må rettighetene tolkes og tilpasses dagens virkelighet. Da EMK ble vedtatt i 1950 eksisterte eksempelvis ikke den teknologien vi operer med i dagens samfunn.

Høyesterett har lagt til grunn at norske rettsanvendere skal foreta en selvstendig tolkning av EMK og benytte samme metode som EMD.³⁹ Herunder at norske domstoler skal forholde seg til «konvensjonsteksten, alminnelige formålsbetraktninger og konvensjonsorganenes avgjørelser», jf. Rt. 2000 s. 996 P (Bøhler) på side 1007. Videre må det utvises forsiktighet ved formålsbetraktninger når det ikke foreligger EMD-dommer som ligger nært opp mot tilfellet.⁴⁰

En særskilt metodisk problemstilling ved denne avhandlingen er at EMD ikke direkte har behandlet spørsmålet om myndighetenes adgang til innhenting, lagring og behandling av

³² Jf. ordlyden «De høye Kontraherende Parter» i EMK artikkel 1.

³³ Tilleggsprotokoll 15 trådte i kraft 1. august 2021.

³⁴ Ola Johan Settem, «Subsidiaritetsprinsippet og skjønnsmarginen i EMK-retten» *Jussens Venner*, 30. juni 2016, pp. 119-141.

³⁵ Se *Centrum för rättvisa* 262 følgende og *Big Brother Watch* avsnitt 348 følgende.

³⁶ Vienna Convention on the Law of Treaties, 23. mai 1969 (Wien-konvensjonen).

³⁷ Se eksempelvis *Golder mot Storbritannia* [P] 1975, no. 4451/70 avsnitt 29.

³⁸ *Tyrer mot Storbritannia* [J] 1978, no. 5856/72 avsnitt 31.

³⁹ Jf. eksempelvis Rt. 2005 s. 833 A avsnitt 45 og Rt. 2008 s. 1409 S avsnitt 74.

⁴⁰ Ola Mestad «Rettens kilder og anvendelse» i Alf Petter Høgberg (red.) og Jørn Øyrehagen Sunde (Red.), *Juridisk metode og tenkemåte*, Universitetsforlaget 2019, side 101-102.

åpent tilgjengelig informasjon etter EMK artikkel 8. I Rt. 2005 s. 833 A kom Høyesterett i storkammer med generelle uttalelser om tolkningen av EMK. Saken omhandlet uskyldspresumpsjonen etter EMK artikkel 6 nr. 2, og gjaldt et tilfelle som EMD ikke hadde behandlet. Høyesterett la til grunn at dersom det er «tvil om betydningen av EMDs avgjørelser vil det ha vekt om saksforholdet kan jevnføres med det som foreligger til avgjørelse i norsk rett.» Hvorvidt det ikke foreligger praksis fra EMD om det gjeldende spørsmålet, utelukker det «ikke at det kan trekkes bindende slutninger fra EMDs praksis til vår sak.»⁴¹

Selv om det ikke foreligger praksis fra EMD som har vurdert lovligheten til myndighetenes masseinnsamling, lagring og analysering av åpent tilgjengelig informasjon, har EMD behandlet flere saker hvor myndighetenes overvåking og bruk av teknologi har vært tema. Følgelig skal det ved usikkerhet vedrørende spørsmålet som behandles, og om EMDs praksis er overførbart, vurderes om det kan jevnføres med det foreliggende tilfellet. EMDs fremgangsmåte og konklusjon i saker som gjelder overvåking vil derfor kunne ha overføringsverdi til problemstillingen i denne avhandlingen.

1.4 Avgrensninger og fremstillingen videre

Retten til privatliv er vernet av Grunnloven⁴² § 102, EMK artikkel 8 og SP artikkel 17. EU-retten inneholder også regler om personvern som Law Enforcement Directive⁴³ som regulerer politiets og påtalemyndighetenes behandling av personopplysninger. Grunnloven § 102 er inspirert av EMK artikkel 8.⁴⁴ Høyesterett har lagt til grunn at grunnlovsbestemmelsen må tolkes med utgangspunkt i den tilsvarende bestemmelsen i EMK.⁴⁵ Det er avsagt nyere avgjørelser fra EMD som omhandler spørsmålet om myndighetenes adgang til å overvåke borgerne med teknologiske verktøy.⁴⁶ Norske domstoler har ikke behandlet spørsmål om masseinnsamling av opplysninger ved hjelp av teknologiske virkemidler. Derfor skal det fokuseres på EMK artikkel 8 ved retten til privatliv i denne avhandlingen. EMD henviser

⁴¹ Rt. 2005 s. 833 A avsnitt 47.

⁴² Kongeriket Norges Grunnlov, Lov 17. mai 1814.

⁴³ Europaparlaments- og rådsdirektiv (EU) 2016/680.

⁴⁴ Se eksempelvis HR-2020-2372-A avsnitt 38.

⁴⁵ Se Rt. 2015 s. 93 A (Maria) avsnitt 57, Rt. 2015 s. 155 A (Rwanda) avsnitt 40, og HR-2016-2554-P (Holship) avsnitt 81.

⁴⁶ Eksempelvis *Centrum för rättvisa* og *Big Brother Watch*.

iblant i sine avgjørelser til EØS-retten og praksis fra EU-domstolen, men for denne avhandlingen vil det avgrenses mot EØS-rett på grunn av plasshensyn.

Utover å vurdere om det foreligger et inngrep som aktualiserer EMK artikkel 8, vil ikke denne avhandlingen gå nærmere inn på de prosessuelle sidene som eksempelvis søksmålsadgang. Dette faller utenfor oppgavens hovedtema. Det skal heller ikke utdypes detaljert om teknologiske verktøy. Informasjon om teknologiske verktøy skal holdes på et overordnet nivå.

Angående teknologiske begreper vil «bulkinnsamling» og «masseinnsamling» brukes om systemet for teknologisk innhenting av store mengder data. «Selektorer» vil i denne avhandlingen være betegnelsen på søkebegreper som brukes i teknologiske systemer for å velge ut datainformasjon. Eksempelvis kan et datasystem tillegges selektorer som velger informasjon til innhenting eller behandling. Begrepene «informasjon» og «opplysninger» vil i denne avhandlingen brukes synonymt om data som innhentes, lagres og behandles. Det vil ikke skilles mellom eksempelvis innholdsdata og metadata.

Høringsnotatet om politiregisterloven § 65 a inneholder flere endringer i politiloven, politiregisterloven og politiregisterforskriften. Avhandlingen skal i utgangspunktet behandle forslag til politiregisterloven § 65 a. Det skal dermed ikke gis en grundig redegjørelse av alle aspekter vedrørende høringsnotatet. Imidlertid vil de øvrige endringene som fremgår av høringsnotatet fremlegges der det er nødvendig for et helhetlig bilde av bestemmelsen.

Begge hovedproblemstillingene besvares samlet i avhandlingen. Den videre fremstillingen disponeres etter EMK artikkel 8 og EMDs fremgangsmåte. EMDs metode i saker som gjelder masseinnsamling av informasjon tilsier en vurdering i to ledd. Først må det tas stilling til om det foreligger et inngrep i EMK artikkel 8 (kapittel 3). I bekreftende fall må det dernest tas stilling til hvilke krav det skal stilles til rettsgrunnlaget for at inngrepet er rettmessig. I rettmessighetsvurderingen inngår vilkårene om at inngrepet må forfølge et legitimt formål, være «in accordance with the law» og «necessary in a democratic society», jf. EMK artikkel 8 nr. 2. Det er nær sammenheng mellom disse vurderingene. I denne avhandlingen vil imidlertid legitimt formål behandles i et eget kapittel (kapittel 4). Vilkårene «in accordance with the law» og «necessary in a democratic society» behandles samlet i kapittelet «Rettmessighet» (kapittel 5). Avslutningsvis vil det foretas en rettspolitisk betraktning (kapittel 6).

Avhandlingen er i et spenningsforhold mellom retten til privatliv og myndighetenes beskyttelse av nasjonal sikkerhet. Innledningsvis skal det dermed klarlegges nærmere om viktigheten av retten til privatliv (kapittel 2). Angående myndighetenes beskyttelse av nasjonal sikkerhet skal viktigheten av dette fremheves i kapittelet om legitimt formål (kapittel 4).

2 Generelt om retten til privatliv

I dette kapittelet skal viktigheten av retten til privatliv belyses. Dette for å sette avhandlingens perspektiv på retten til privatliv, og gi et bilde av konsekvensene av å ikke ha en slik rettighet.

Det fremgår av EMK artikkel 8 nr. 1 at enhver har rett til «respect for his private and family life, his home and his correspondence». Ordlyden gir en vid angivelse av rettigheten. Retten til privatliv omfavner retten til familieliv, hjem og korrespondanse, og derfor kan rettighetene ofte overlappe hverandre, uten at dette vil ha avgjørende betydning.⁴⁷ Retten til privatliv beskytter individer som er direkte berørt av statens tiltak. Dette gjelder også i tilfeller der myndighetenes tiltak er rettet mot den bredere befolkning,⁴⁸ og juridiske personer⁴⁹ ved «home» og «correspondence».

Retten til privatliv har ingen uttømmende definisjon.⁵⁰ EMD har uttalt at rettigheten må tolkes vidt. Retten til privatliv er en forutsetning for individets utvikling, og nødvendig for å kunne etablere relasjoner til andre.⁵¹ Høyesterett har fremhevet at «sentralt i den foreliggende praksis fra EMD står blant annet menneskets fysiske og psykiske integritet, alle de ulike elementene i den enkeltes identitet i videste forstand og den personlige autonomi», jf. Rt. 2015 s. 93 A. EMD har lagt til grunn at konvensjonsbestemmelsen inneholder en rett til vern av personopplysninger.⁵² Dersom myndighetene behandler en opplysning som kan identifisere et individ vil dette være vernet av EMK artikkel 8.⁵³

⁴⁷ Se eksempelvis *Big Brother Watch og Centrum för rättvisa*.

⁴⁸ Se eksempelvis *Klass og andre mot Tyskland* [P] 1978, no. 5029/71.

⁴⁹ Se eksempelvis *Association for European Integration and Human Rights og Ekimdzhev mot Bulgaria* [J] 2007, no. 62540/00 avsnitt 60.

⁵⁰ Eksempelvis *Gillan and Quinton mot Storbritannia* [J] 2010, no. 4158/05 avsnitt 61.

⁵¹ *Jehovah's Witnesses of Moscow og andre mot Russland* [J] 2010, no. 302/02 avsnitt 117.

⁵² Se eksempelvis *Rotaru mot Romania* [J] 2000, no. 28341/95 avsnitt 43.

⁵³ *Amann mot Sveits* [J] 2000, no. 27798/95 avsnitt 65.

Korrespondansevernet innebærer at enhver skal kunne utfolde seg selv og sine meninger, og delta i den demokratiske debatten. Korrespondanse omfatter kommunikasjon, eksempelvis ved telefon, brev eller e-post.⁵⁴ På denne måten inneholder rettigheten en beskyttelse mot eksempelvis urettmessig kommunikasjonskontroll, overvåking og avlytting. Retten til privatliv henger dermed nært sammen med ytringsfriheten, som også er en beskyttet menneskerettighet.⁵⁵ Ytringsfriheten er individers rett til å uttrykke seg, og et inngrep i retten til privatliv kan påvirke ytringsfriheten. Dersom handlingsrommet for privatlivet blir innskrenket kan det ha en nedkjølende effekt på individers ytringer.⁵⁶

I offentlig utredning fra 2009 skrev metodekontrollutvalget at «den private sfære er (...) en forutsetning for menneskets dannelsesprosess og myndiggjøring, samt for demokratiet og maktbalansen».⁵⁷ Dette betyr at begrunnelsen for å beskytte retten til privatliv ikke bare er individuelt begrunnet, men at det også er viktig fra et samfunnsperspektiv. I saker som gjelder overvåking hvor retten til privatlivet har blitt truet, har EMD ved flere anledninger lagt til grunn et følgende prinsipielt utgangspunkt: «the risk that a system of secret surveillance set up to protect national security may undermine or even destroy democracy under the cloak of defending it».⁵⁸ Et kontrollsamfunn der staten har tilgang til all informasjon om borgerne, kan svekke tilliten blant befolkningen og samtidig øke risikoen for myndighetsmisbruk. Et strengt personvern er derfor en forutsetning for samfunnets maktfordeling og for demokratiet i sin helhet.⁵⁹

Sammenfattet kan man si at retten til privatliv verner mot innblanding fra myndighetene, i dette tilfellet PST, i den private sfære.

⁵⁴ Jørgen Aall, *Rettsstat og menneskerettigheter*, 5. utgave, Fagbokforlaget 2018, s. 252.

⁵⁵ Se Grunnloven § 100 og EMK artikkel 10.

⁵⁶ Dette var tilfellet i eksempelvis *Silver og andre mot Storbritannia* [J] 1983, nos. 5947/72, 6205/73, 7052/75, 7061/75, 7107/75, 7113/75, 7136/75 avsnitt 85.

⁵⁷ Jf. NOU 2009: 15 Skjult informasjon – åpen kontroll, s. 51.

⁵⁸ *Roman Zakharov mot Russland* [GC] 2015, no. 47143/06 avsnitt 232, *Szabó og Vissy mot Ungarn* [J] 2016, no. 37138/14 avsnitt 57, *Weber og Saravia mot Tyskland* [J] 2006, no. 54934/00 avsnitt 106, *Centrum för rättvisa* avsnitt 253, og *Big Brother Watch* avsnitt 339.

⁵⁹ NOU 2009: 15 Skjult informasjon – åpen kontroll, s. 51.

3 Inngrep

3.1 Introduksjon

Forslaget til PSTs adgang til innhenting, lagring og behandling av åpent tilgjengelig informasjon etter politiregisterloven ny § 65 a inneholder forhold som vil berøre retten til privatliv. I dette kapittelet skal det vurderes i hvilken grad det utgjør et inngrep i EMK artikkel 8. EMD har behandlet en rekke ulike saker om lovligheten av myndighetenes skjulte informasjonsinnhenting av borgerne som skal hensyntas i denne vurderingen.

Innledningsvis skal det gjøres rede for generelle utgangspunkter ved inngrepsvurderingen. Herunder skal det med utgangspunkt i EMDs fremgangsmåte ved inngrepsvurderingen i *Big Brother Watch* og *Centrum för rättvisa*, vurderes i hvilken grad denne fremgangsmåten gjør seg gjeldende for PSTs adgang til innhenting, lagring og behandling av åpent tilgjengelig informasjon. Deretter skal det klarlegges hva som inngår i «åpent tilgjengelig informasjon» etter forslaget og inngrepsgraden knyttet til dette. Til sist skal det vurderes i hvilken grad det utgjør et inngrep i EMK artikkel 8 i tråd med EMDs prinsipper, hvor inngrepet tiltar underveis i prosessen.

3.2 Arten av inngrepet, hvordan det rammer og hvor tyngende det er overfor den som rammes

3.2.1 Rettslige utgangspunkter

Bruk av informasjon som er tilgjengelig i det offentlige er i utgangspunktet ikke et inngrep i privatlivet.⁶⁰ I utgangspunktet kan enhver observere en annen person på offentlig sted. På grunn av legalitetsprinsippet kan likevel ikke handlingsrommet til private personer og offentlige myndigheter likestilles. En privatperson som observerer en annen vil ikke være omfattet av legalitetsprinsippet, i motsetning til staten som utøver offentlig myndighet. Dette er fordi utøvelse av offentlig myndighet ved «inngrep overfor den enkelte må ha grunnlag i lov», jf. Grunnloven § 113, mens en privatperson i utgangspunktet kan handle fritt. Dette gjelder imidlertid til en viss grense fordi en privatperson kan rammes av et straffebud ved eksempelvis å forfølge en annen, jf. straffeloven⁶¹ § 266. Det synes lagt til grunn av

⁶⁰ *Uzun mot Tyskland* [J] 2010, no. 35623/05 avsnitt 44.

⁶¹ Lov 20. mai 2005 nr. 28 om straff (straffeloven – strl.).

Politimetodeutvalget i NOU 2004:6 at «[å] iaktta og trekke slutninger på grunnlag av det observerte, er allmennmenneskelig atferd som alle og enhver kan gjennomføre».⁶²

EMD har i flere avgjørelser lagt til grunn at informasjon i den offentlige sfære kan utgjøre et inngrep i retten til privatliv.⁶³ I *Rotaru mot Romania* ble det lagt til grunn at offentlig informasjon kan utgjøre et inngrep dersom det er systematisk innhentet og lagret av offentlige myndigheter, særlig dersom informasjonen fra vedkommende ligger langt tilbake i tid ("distant past").⁶⁴ Det fremgår av avgjørelsen *P.G. og J.H. mot Storbritannia* at selv om offentlig tilgjengelig informasjon ikke er innhentet ved inngripende eller skjulte metoder, kan det utgjøre et inngrep når myndighetene systematisk innhenter og permanent lagrer informasjonen. I denne relasjon ble det lagt til grunn at vedkommendes forventninger til privatlivet er av betydning, men ikke avgjørende.⁶⁵

Masseinnhenting, lagringstiden på 15 år og den systematiske behandlingen av informasjonen er klart et inngrep i EMK artikkel 8 etter EMDs praksis. Dette har også departementet lagt til grunn i høringsnotatet.⁶⁶ Videre er spørsmålet hvor stort inngrep masseinnsamling og etterfølgende behandling av opplysningene utgjør i EMK artikkel 8.

Departementet fremholder at åpent tilgjengelig informasjon skiller seg vesentlig fra tilrettelagt innhenting, bruk av skjulte tvangsmidler og andre inngripende overvåkningsmetoder.⁶⁷

Argumentet ble brukt mot overføringsverdien av to nylig avsatte kammeravgjørelser fra EMD om bulkinnsamling, henholdsvis *Big Brother Watch* og *Centrum för rättvisa*. Faktumet i dommene handlet i korte trekk om at etterretningstjenestene innhentet grensekryssende kommunikasjonsdata i bulk. Dette gjaldt all informasjon som krysset landegrensene.

I avgjørelsene ble det lagt til grunn stadier i en bulkinnsamlingsprosess som har betydning for hvor inngripende tiltaket er:

“(a) the interception and initial retention of communications and related communications data (that is, the traffic data belonging to the intercepted communications);

⁶² NOU 2004: 6 Mellom effektivitet og personvern: Politimetoder i forebyggende øyemed, i avsnitt 7.2.3.3.

⁶³ Se eksempelvis *Rotaru mot Romania* [J] 2000, no. 28341/95 avsnitt 43, *P.G. og J.H. mot Storbritannia* [J] 2001, no. 44787/98 avsnitt 5, og *Gillan og Quinton mot Storbritannia* [J] 2010, no. 4158/05 avsnitt 61.

⁶⁴ *Rotaru mot Romania* [J] 2000, no. 28341/95 avsnitt 43.

⁶⁵ *P.G. og J.H. mot Storbritannia* [J] 2001, no. 44787/98 avsnitt 57.

⁶⁶ Høringsnotatet punkt 5.2.2.

⁶⁷ Høringsnotatet punkt 3.4.1.2.

- (b) *the application of specific selectors to the retained communications/related communications data;*
- (c) *the examination of selected communications/related communications data by analysts;*
and
- (d) *the subsequent retention of data and use of the “final product”, including the sharing of data with third parties.”*⁶⁸

EMD har lagt til grunn at ethvert steg i denne prosessen kan utgjøre et inngrep i EMK artikkel 8. Det første steget er mindre inngripende enn de øvrige, men inngrepsgraden tiltar underveis i bulkinnsamlingsprosessen.⁶⁹ Inngrepsgraden vil samtidig ha betydning for om forslaget inneholder tilstrekkelige rettssikkerhetsmekanismer og således er rettmessig.

EMD knytter generelle uttalelser til denne fremgangsmåten, slik at det skal gjelde for ulike former for masseinnsamling. Herunder uttales det at det aksepteres at ikke alle systemer med masseinnsamling følger nøyaktig samme modell.⁷⁰ Med dette forbehold oppstiller EMD en generell fremgangsmåte for å vurdere inngrepsgraden av bulkinnsamlingssystemer.⁷¹ Dermed er EMDs kriterier for å vurdere inngrepet av masseinnsamling generelt formulert. Fremgangsmåten er ikke begrenset til å gjelde innhenting av individuell kommunikasjonsdata, men også andre former for masseinnhenting. Dermed er konklusjonen så langt at EMDs praksis på dette området også må kunne anvendes for masseinnsamling av åpne kilder.

3.2.2 Generelt om inngrepsgrad vedrørende «åpent tilgjengelig informasjon»

Det fremgår av forslaget at det skal innhentes «åpent tilgjengelig informasjon». I forslaget defineres åpent tilgjengelig informasjon som «informasjon som er allment tilgjengelig for offentligheten.»⁷² Dermed at alt som publiseres i det åpne rom på internettet er gjenstand for innhenting, lagring og behandling av PST. Videre mener departementet at informasjon som publiseres på lukkede nettsteder eller private samtaler ikke omfattes av lagringen.⁷³

⁶⁸ *Centrum för rättvisa* avsnitt 239 og *Big Brother Watch* avsnitt 325.

⁶⁹ *Centrum för rättvisa* avsnitt 244 og *Big Brother Watch* avsnitt 330.

⁷⁰ *Centrum för rättvisa* avsnitt 239 og *Big Brother Watch* avsnitt 325.

⁷¹ *Centrum för rättvisa* avsnitt 239 og *Big Brother Watch* avsnitt 325.

⁷² Høringsnotatet punkt 1.

⁷³ Høringsnotatet punkt 5.2.3.

Ordlyden av «åpent tilgjengelig informasjon» tilsier at det er informasjon som er tilgjengelig for enhver uten at det kreves en ytterligere handling for å få tak i informasjonen. Hvorvidt et nettsted kan anses som offentlig tilgjengelig, fremholder departementet at det «vil bero på om og i hvilken grad det utøves en reell kontroll med tilgangen til nettstedet.»⁷⁴ Ut ifra denne formuleringen fremstår det som om det ikke kreves en ytterligere handling for å få tak i informasjonen. Imidlertid fortsetter departementet med at dersom det kreves registrering, abonnement eller at det må opprettes en bruker for å få tilgang til informasjonen, regnes dette som åpent tilgjengelig informasjon.⁷⁵

Dermed er det noen uklarheter ved avgrensningen av «åpent tilgjengelig informasjon». Fra den forutgående fremleggelsen av EMDs praksis fremgår det at vedkommendes forventninger til privatlivet skal hensyntas ved vurderingen. Det er ulike grader av om avsenderen mener at innholdet skal tilgjengeliggjøres for offentligheten. En person kan eksempelvis ha ulike forventninger til å publisere et debattinnlegg i en avis, og publikasjon på en privatprofil på «Instagram» eller en privat gruppe på «Facebook».

Departementet legger frem at kammeravgjørelsene ikke er direkte overførbar til behandling av åpent tilgjengelig informasjon fordi de omhandler en annen og mer inngripende form for masseinnhenting.⁷⁶ *Centrum för rättvisa* og *Big Brother Watch* omhandlet innhenting og lagring av kommunikasjon i bulk og etterfølgende søk ved selektorer som identifiserer informasjon.⁷⁷ Informasjonen som ble innhentet kunne være tekst, bilder eller lyd.⁷⁸ Dette innebærer at innhenting inneholdt privat kommunikasjon. Det fremstår som om tilfellene av overvåkning departementet sikter til som mer inngripende, er innhenting av privat og lukket kommunikasjon. Denne kommunikasjonen foregår typisk på lukkede kommunikasjonstjenester, som kun er ment for avsender og mottaker. Eksempelvis er lukket kommunikasjon e-postkorrespondanse. Det kan være mellom flere avsendere og mottakere, men hovedpoenget er at kommunikasjonen kun skal være tilgjengelig for denne avgrensede gruppen.

⁷⁴ Høringsnotatet punkt 5.2.3.

⁷⁵ Høringsnotatet punkt 5.2.3.

⁷⁶ Høringsnotatet punkt 3.4.1.2 og punkt 5.2.6.

⁷⁷ *Centrum för rättvisa* avsnitt 14 og *Big Brother Watch* avsnitt 15 til 19.

⁷⁸ *Centrum för rättvisa* avsnitt 14.

Det kan regnes som at selve innholdet i lukket kommunikasjon i større grad kan inneholde sensitive personopplysninger. Etter EMDs avgjørelser om EMK artikkel 8 er det fremlagt sensitive kategorier av personopplysninger som er særskilt vernet. Sensitive kategorier av personopplysninger er blant annet data som inneholder et individs etniske identitet,⁷⁹ politiske meninger, religiøs trosretning, filosofiske meninger,⁸⁰ og helse, seksuell liv eller seksuell orientering.⁸¹ Det er imidlertid gjort unntak fra politiregisterloven § 7 om sensitive personopplysninger ved PSTs innhenting, lagring og behandling av åpent tilgjengelig informasjon, jf. politiregisterloven ny § 65 a første ledd.⁸² Politiregisterloven § 7 handler om behandling av særlige kategorier av personopplysninger, eksempelvis politisk eller religiøs overbevisning, og seksuell orientering. Uavhengig av om det er gjort unntak, vil innhenting og lagring av såkalte sensitive opplysninger fortsatt medføre at inngrepsgraden forhøyes. Dermed kan åpent tilgjengelig informasjon som PST innhenter, lagrer og behandler inneholde opplysninger som er av intim og sensitiv karakter.

Enkeltpersoners forventninger til privatlivet er klart høyere når det gjelder lukket kommunikasjon. Det kan imidlertid ligge informasjon på det åpne internett som andre har publisert om deg, som du ikke er klar over eller ikke har samtykket til. Et eksempel er at noen med uhell publiserer sensitive opplysninger på det åpne nett, og deretter sletter det etter publisering. Eller at cyberkriminelle utfører et angrep og publiserer privat informasjon, som eksempelvis private bilder på forumer. Tross at intensjonen ikke var offentlighet, kan opplysningene likevel bli innhentet av PST. Når man ser på eksemplene om at det ikke tas forbehold om personopplysninger som aldri var ment å bli publisert i det åpne rom, eller at andre deler personsensitiv informasjon om en annen - kan innholdet, potensielt sett, være av tilsvarende sensitiv karakter som ved lukket kommunikasjon. Det må dermed legges til grunn at det innhentede innholdet kan være av betydelig inngripende karakter også ved åpent tilgjengelig informasjon.

Som lagt frem ovenfor er offentlig informasjon inngripende dersom det er systematisk innhentet og lagret over lengre tid av myndighetene. Inngrepsgraden tiltar som sagt tidligere underveis i prosessen, og inngrepet vil ytterligere økes dersom opplysningene blir underlagt

⁷⁹ Se *S. and Marper mot Storbritannia* [GC] 2008, nos. 30562/04 og 30566/04 avsnitt 66, og *Ciubotaru mot Moldova* [J] 2010, no. 27138/04 avsnitt 49.

⁸⁰ Eksempelvis *Catt mot Storbritannia* [J] 2019, no. 43514/15 avsnitt 112.

⁸¹ Eksempelvis *Mockutė mot Litauen* [J] 2018, no. 66490/09 avsnitt 94.

⁸² Høringsnotatet punkt 7.2.

nærmere analyse.⁸³ Følgelig må graden av inngrepet i den private sfære ved informasjon fra åpne kilder sammenholdes med hvilken behandling det blir utsatt for.

3.2.3 Innhenting og den innledende oppbevaringen av data

Det første stadiet i en bulkinnsamlingsprosess, punkt (a)⁸⁴, omhandler at innhenting av elektronisk kommunikasjonsdata foretas i store mengder. Dette gjelder også informasjon som vil være av mindre interesse for sikkerhetstjenestene.⁸⁵ Det fremgår lite informasjon i høringsnotatet om selve innhenting av åpent tilgjengelig informasjon. Det fremgår kun at det kan foretas masseinnhenting av informasjon fra åpne kilder.⁸⁶ Det er imidlertid på samme måte som i *Big Brother Watch* og *Centrum för rättvisa* masseinnhenting av informasjon som ikke er systematisk eller rettet mot et konkret individ, og at innhenting kan omfatte informasjon som ikke er av interesse for PSTs oppgaveløsning.⁸⁷

Innhenting av åpent tilgjengelig informasjon er mindre inngripende enn innhenting av lukket kommunikasjon. Dette fordi det blir «effected outside a person's home or private premises».⁸⁸ Myndighetene trenger ikke inn i kommunikasjon på samme måte som de tilfellene som er ment lukket, eksempelvis meldinger sendt som SMS eller e-post mellom privatpersoner. Etersom kommunikasjonen er privat, har enkeltpersoner en høyere forventning til privatlivet. Dette tyder på at det innledende stadiet ved åpent tilgjengelig informasjon, selv om det utgjør et inngrep, er mindre inngripende enn innhenting av lukket og privat kommunikasjon.

Foreløpig konklusjon er derfor at innhenting av åpent tilgjengelig informasjon utgjør et inngrep, men er mindre inngripende enn tilfellene i de fremlagte kammeravgjørelsene fra EMD.

3.2.4 Behandling av det innhentede materialet

Punkt (b) i EMDs inngrepsvurdering handler om søk i det innhentede materialet som for det meste er automatisert, og som kan innebære søk mot enkeltpersoner.⁸⁹ I punkt (c) forhøyes

⁸³ *Centrum för rättvisa* avsnitt 244-245 og *Big Brother Watch* avsnitt 330-331.

⁸⁴ *Centrum för rättvisa* avsnitt 239 og *Big Brother Watch* avsnitt 325.

⁸⁵ *Centrum för rättvisa* avsnitt 240 og *Big Brother Watch* avsnitt 326.

⁸⁶ Høringsnotatet punkt 3.4.1.

⁸⁷ Høringsnotatet punkt 5.2.2.

⁸⁸ *Uzun mot Tyskland* [J] 2010, no. 35623/05 avsnitt 44.

⁸⁹ *Centrum för rättvisa* avsnitt 241 og *Big Brother Watch* avsnitt 327.

inngrepet ytterligere ved at det innhentede materialet blir vurdert nærmere ved menneskelig behandling.⁹⁰

PSTs behandling av åpent tilgjengelig informasjon kan foregå helt eller delvis ved automatiserte analyseverktøy, eller på annen måte etter politiregisterloven ny § 65 a.⁹¹ Ved bruk av ulike maskinlæringssystemer og kunstig intelligens kan det hentes ut mye informasjon fra åpne kilder. Eksempelvis kan mental helsetilstand estimeres ved bruk av data fra sosiale medier⁹² og ut ifra bilder kan en persons seksuelle legning anslås⁹³. Elektronisk behandling av data kan i seg selv være svært inngripende. EMD la til grunn i *Centrum för rättvisa* og *Big Brother Watch* at når informasjon lagres i store mengder er det gjenstand for nærmere analyse og undersøkelser som kan sette sammen et intimt bilde av enkeltpersoner.⁹⁴ Dette gjelder uavhengig av om innholdet blir nærmere undersøkt av en fysisk person.

Inngrepet blir sterkere desto mer filtrert og rettet analysen av materialet er.⁹⁵ Det blir ikke informert i høringsnotatet om hvilke analyseverktøy som vil brukes, hvordan det vil benyttes eller fra hvilke leverandører. Det eneste som fremgår er at det vil medføre behov for modernisering eller utvikling av IKT-systemer.⁹⁶ I skriftlig spørsmål fra Guri Melby, politiker i partiet Venstre, til daværende forsvarsminister Odd Roger Enoksen ble det stilt spørsmål om leverandører som var aktuelle for å opprette systemet ved Etterretningstjenestens bulklagringsregime om grenseoverskridende elektronisk kommunikasjon. Forsvarsministeren besvarte spørsmålet med at aktuelle leverandører ikke kunne offentliggjøres grunnet skjermings- og konkurransehensyn, og av hensyn til kommende kontraktsforhandlinger ville ikke Forsvarsdepartementet gi nærmere innsyn i prosjektinformasjonen.⁹⁷ Dette omhandler ikke PSTs adgang til masseinnsamling av åpent tilgjengelig informasjon, men det kan legges til grunn at det er samme begrunnelse også her. Av hensyn til det offentlige

⁹⁰ *Centrum för rättvisa* avsnitt 242 og *Big Brother Watch* avsnitt 328.

⁹¹ Høringsnotatet punkt 5.2.4 og 7.3.

⁹² Chancellor, S., De Choudhury, M. Methods in predictive techniques for mental health status on social media: a critical review. *npj Digit. Med.* 3, 43 (2020), <https://doi.org/10.1038/s41746-020-0233-7> (lest 17.02.2022).

⁹³ Leuner, John, A Replication Study: Machine Learning Models Are Capable of Predicting Sexual Orientation From Facial Images (2019), <https://arxiv.org/abs/1902.10739> (lest 17.02.2022).

⁹⁴ *Big Brother Watch* avsnitt 330.

⁹⁵ *Centrum för rättvisa* avsnitt 256 og *Big Brother Watch* avsnitt 342.

⁹⁶ Høringsnotatet punkt 6.

⁹⁷ Skriftlig spørsmål fra Guri Melby (V) til forsvarsministeren, https://www.stortinget.no/no/Saker-og-publikasjoner/Sporsmal/Skriftlige-sporsmal-og-svar/Skriftlig-sporsmal/?qid=86975&fbclid=IwAR1gwEuST2d6eLJbuHZBY6sO_JOICvTq1BSfrWg0hKmV6KopgAS4nQy-iH0 (lest 09.02.2022).

forhandlingsposisjon gis det ikke nærmere informasjon om IKT-systemene som skal brukes. Problematikken ved å ikke få opplyst hvilke verktøy som brukes knytter seg til hvordan innholdet analyseres. Det er hvordan slik informasjon analyseres som kan ha et skadepotensiale og derav kan være mer inngripende. Konsekvensen er at analysene kan utvinne personopplysninger som enkeltmennesker ikke har valgt å publisere.

Som vist til tidligere skal det ved forslag til politiregisterloven § 65 a gjøres unntak fra lovens § 7 om behandling av særlige kategorier av personopplysninger. Dette er personlig informasjon som er særskilt vernet.⁹⁸ Ved bruk av analyseverktøy på åpne kilder kan denne informasjonen enkelt kategoriseres. I eksempelvis *Centrum för rättvisa* var det ved bulkinnsamlingssystemet et forbud mot å kun behandle slik informasjon, som ble ansett som en positiv avgrensning av EMD.⁹⁹ En ytterligere problematikk knyttet til dette er at opplysningene som blir behandlet, ikke nødvendigvis er opplysninger vedkommende selv har valgt å publisere. Videre legger forslaget opp til at informasjon som er uriktig eller utdatert også kan behandles, ettersom det er gjort unntak fra politiregisterloven § 6. Ved lengste lagringstid på 15 år kan det potensielt risikere at det behandles informasjon som er både uriktig og fra et individs «distant past».¹⁰⁰

Den innhentede informasjonen kan også bli utsatt for menneskelig behandling i PST. Informasjonen skal sperres,¹⁰¹ og de som gis tilgang til opplysningene skal begrenses til så få personer som mulig, og bare gis til personer som har særskilt bemyndigelse til dette.¹⁰²

Følgelig er det likhetstrekk ved PSTs adgang til behandling av åpent tilgjengelig informasjon og behandlingen av informasjon i *Big Brother Watch* og *Centrum för rättvisa*. Herunder at behandlingen kan foregå med automatiserte verktøy og at det innhentede materialet kan bli vurdert nærmere ved menneskelig behandling.

⁹⁸ Se punkt 3.2.2.

⁹⁹ *Centrum för rättvisa* avsnitt 314.

¹⁰⁰ Jf. ovenfor, *Rotaru mot Romania* [GC] 2000, no. 28341/95 avsnitt 43.

¹⁰¹ Jf. politiregisterloven ny § 65 a annet ledd.

¹⁰² Jf. høringsnotat punkt 7.3 om politiregisterforskriften ny § 21-8 første ledd.

3.2.5 Påfølgende oppbevaring av data og deling med andre

EMD viser til at punkt (d) omhandler den siste fasen hvor informasjonen blir brukt av etterretningstjenesten. Dette kan innebære å fremstille en rapport, deling av informasjonen til andre nasjonale organer, eller utenlandske etterretningstjenester.¹⁰³

Det følger av Instruks om Politiets sikkerhetstjeneste § 6 første ledd at PSTs sentrale enhet skal «utarbeide trusselvurderinger og gi råd i tiltak av betydning for norske interesser, virksomheter og enkeltpersoners sikkerhet». Ved PSTs forbyggende oppgaver skal det blant annet innhentes, bearbejdes, analyseres og utveksles informasjon, jf. Instruks for Politiets sikkerhetstjeneste § 5 første ledd. PST skal samarbeide nasjonalt med Politidirektoratet, Etterretningstjenesten og Nasjonal sikkerhetsmyndighet, jf. Instruks for Politiets sikkerhetstjeneste § 10 første ledd første punktum. PST skal også samarbeide med andre lands etterretnings- og sikkerhetsmyndigheter, jf. Instruksen § 11 første ledd.

PSTs adgang til bruk av åpent tilgjengelig informasjon er ikke begrenset til etterretningsformål. Etter politiregisterloven ny § 65 a annet ledd kan det også brukes til forebyggende sak eller etterforskning. Behandlingen av åpne kilder kan dermed gjennomføres for alle de tre formålene til PST. Ettersom opplysningene kan brukes til etterforskning, vil behandlingen potensielt innebære et langt større personvernsinngrep, enn ved kun etterretningsformål. Dette viser til at behandling og bruk av åpne kilder er mer inngripende enn det departementet har lagt til grunn i høringsnotatet.

Angående den videre oppbevaringen av informasjon, er lengstefristen for sletting 15 år. EMD har lagt til grunn at lagring av data som relaterer til privatlivet til et individ, også isolert sett, utgjør et inngrep i EMK artikkel 8.¹⁰⁴ Det foretas unntak fra politiregisterloven § 6 som omhandler opplysningenes kvalitet hvorav opplysningene skal være tilstrekkelige og relevante, korrekte og oppdaterte, og ikke lagres lengre enn nødvendig, jf. bestemmelsens første ledd nr. 1 til 3. I løpet av 15 år kan informasjonen bli utdatert og eksempelvis gi et feilaktig bilde av vedkommende. Dessuten er det uklart hvordan teknologien utvikles på 15 år, og det er usikkert hvordan denne informasjonen vil brukes om 15 år. Ved masseinnhenting blir det innhentet en rekke informasjon som ikke er relevant for PSTs virksomhet. Slik

¹⁰³ *Centrum för rättvisa* avsnitt 243 og *Big Brother Watch* avsnitt 329.

¹⁰⁴ *Centrum för rättvisa* avsnitt 244, *Big Brother Watch* avsnitt 330, og *Leander mot Sverige* [J] 1987, no. 9248/81 avsnitt 48.

overskuddsinformasjon kan da holdes lagret i 15 år selv om det ikke er nødvendig til formålet.

3.3 Konklusjon

Med utgangspunkt i EMDs fremgangsmåte ved inngrepsvurderingen er innhenting, lagring og behandling av åpent tilgjengelig informasjon etter ny politiregisterloven § 65 a, mer inngripende enn det departementet viser til i forslaget.

Det foreligger svakheter ved å ikke adressere den særskilte problematikken som kan oppstå ved de teknologiske verktøyene som brukes. Ettersom informasjon etter dagens teknologi kan settes sammen, forvaltes og brukes på en annen måte enn tidligere, må dette anses som inngripende forhold. Ved å ikke få innsyn i hvilke maskinlæringsystemer som brukes er det vanskelig å vurdere om den innsamlede informasjonen kan misbrukes. Imidlertid er det tilstrekkelig, ved inngrepsvurderingen, å fastslå at et slikt teknologisk system kan legge opp til misbruk fra myndighetenes side.¹⁰⁵ Forslaget til politiregisterlov § 65 a er mer inngripende desto mer informasjonen blir behandlet og brukt. Dette er forhold som må vurderes av lovgiver ved inngrepsvurderingen etter EMK artikkel 8.

PSTs innledende informasjonsinnhenting er mindre inngripende enn når myndighetene innhenter opplysninger fra lukkede kommunikasjonsformer, som i *Big Brother Watch* og *Centrum för rättvisa*. På den annen side vil den videre behandlingen av opplysningene forhøye inngrepet, og samtidig kreve ytterligere rettssikkerhetsmekanismer. EMD har i disse bulkinnhentingssakene vurdert at inngrepsgraden øker etter at opplysningene er samlet inn. Dette tilsier at rettssikkerhetsmekanismene som EMD oppstiller i *Big Brother Watch* og *Centrum för rättvisa* også bør anvendes når PST samler inn og behandler opplysningene slik det er fremstilt i høringsnotatet.

¹⁰⁵ *Roman Zakharov mot Russland* [GC] 2015, no. 47143/06 avsnitt 232, *Szabó og Vissy mot Ungarn* [J] 2016, no. 37138/14 avsnitt 57, *Weber og Saravia mot Tyskland* [J] 2006, no. 54934/00 avsnitt 106, *Centrum för rättvisa* avsnitt 253, og *Big Brother Watch* avsnitt 339.

4 Legitimt formål

4.1 Utgangspunkter

Når det konstateres et inngrep må det forfølge ett eller flere av de alternative legitime formål som er opplistet i EMK artikkel 8 nr. 2 for å være et rettmessig inngrep. Ordlyden er at “There shall be no interference by a public authority with the exercise of this right except such as is [...] in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.” I rettmessighetsvurderingen er det en avveining av retten til privatliv mot ett eller flere av de nevnte formål.

Begrunnelsen for at det kan gjøres inngrep i retten til privatliv etter særskilte formål, er fordi det aksepteres at myndighetene i enkelte tilfeller gjør unntak fra rettigheten for å ivareta viktige interesser. I EMDs avgjørelser om overvåkning er det lagt til grunn at myndighetene har en vid skjønnsmargin ved ivaretagelse av nasjonal sikkerhet.¹⁰⁶ I avgjørelsene om overvåkning har ikke EMD problematisert vilkåret om å forfølge et legitimt formål.¹⁰⁷ Begrunnelsen må være at det anses som uomtvistet at det er oppfylt.

I det følgende skal det gjøres rede for hvilket legitimt formål som forfølges ved forslaget om PSTs innhenting, lagring og behandling av åpent tilgjengelig informasjon etter politiregisterloven ny § 65 a. Samtidig skal viktigheten av at PST innehar en slik adgang fremheves.

4.2 Hvilket legitimt formål forfølges ved PSTs innhenting, lagring og behandling av åpent tilgjengelig informasjon?

Ettersom samfunnet stadig blir digitalisert har det medført at trusselutøveres aktivitet øker i det digitale rom.¹⁰⁸ På internett kan en eksempelvis komme over ekstreme ytringsforumer hvor det fremmes ekstremistiske ideologier og ideer til terrorplanlegging. Nettekstremisme foregår imidlertid ikke kun på ekstremistiske nettsteder, men er også utbredt på sosiale medier utenfor slike fora.¹⁰⁹

¹⁰⁶ Eksempelvis *Weber og Saravia mot Tyskland* [J] 2006, no. 54934/00 avsnitt 106.

¹⁰⁷ Se eksempelvis *Centrum för rättvisa* avsnitt 279 og *Big Brother Watch* avsnitt 365.

¹⁰⁸ PSTs høringsuttalelse 06.01.2022 til Justis- og beredskapsdepartementet side 1.

¹⁰⁹ Inger Marie Sunde (Red.), «Forebygging av radikalisering og voldelig ekstremisme på internett», Rapport fra Politihøgskolen, 2013, side 9.

I Norge har vi opplevd terrorangrep. Den 22. juli 2011 drepte en høyreekstremist 77 mennesker i Regjeringskvartalet og på Utøya. Av dommen avsagt i Oslo tingrett fremgår det at tiltaltes utvikling av «islamfiendtlige synspunkter blant annet har sammenheng med hans høyreekstremistiske kontakter på Internett», jf. RG-2012-1153 på side 31. I Bærum 10. august 2019 ble det utført et forsøk på terrorhandling med drapsforsøk rettet mot Al-Noor Islamic Centre, og utført et drap på gjerningspersonens stesøster. I dommen fremholdes det at tiltalte over flere år hadde brukt mye tid på internett og i økende grad oppsøkt «nettsider og netttforum med høyreorientert og høyreekstremt innhold», jf. TAHER-2020-5113 (Asker og Bærum tingrett) på punkt 3.

I PSTs Nasjonal trusselvurdering for 2022 fremgår det blant annet at terrortrusselen først og fremst kommer fra personer som er radikaliserert ved høyreekstreme digitale nettverk.¹¹⁰ Digitale plattformer er viktige arenaer for radikalisering og inspirasjon til terrorplanlegging.¹¹¹ I Rapport fra 22. juli-kommisjonen ble det uttrykt en «forventning om at PST skal ‘følge med’ på ekstremistiske nettsider.»¹¹² Vi er avhengige av at PST har tilstrekkelige midler for å ivareta den nasjonale sikkerheten og hindre kriminalitet, for å eksempelvis forhindre terrorangrep.

Begrunnelsen for forslaget til politiregisterloven § 65 a er at PST skal ivareta etterretningsoppdraget som innenlands etterretningstjeneste og kunne «følge med» på internett.¹¹³ PST skal da avdekke ukjente trusselaktører, oppdage fenomener som kan medføre nye trusler og kartlegge utviklingen i trusselbildet.¹¹⁴ Det fremgår av politiregisterloven ny § 65 a annet ledd at den innhentede informasjonen kan brukes til formål om etterretningsvirksomhet, opprettelse av eller bruk i forebyggende sak, og etterforskning. Etterretningsvirksomhet og kriminalitetsbekjempelse er direkte knyttet til formålene om «prevention of disorder or crime» og «national security», jf. EMK artikkel 8 nr. 2. Formålet skal behandles nærmere i kapittel 5.

¹¹⁰ Nasjonal trusselvurdering 2022, PST, side 15.

¹¹¹ Nasjonal trusselvurdering 2021, PST, side 3.

¹¹² Meld. St. 21 (2012–2013) Terrorberedskap — Oppfølging av NOU 2012: 14 Rapport fra 22. juli-kommisjonen, punkt 6.5.7.

¹¹³ Høringsnotatet punkt 1.

¹¹⁴ Høringsnotatet punkt 1.

5 Rettmessighet

5.1 Introduksjon

For at et inngrep i EMK artikkel 8 skal være rettmessig må det forfølge et legitimt formål, være «in accordance with the law» og «necessary in a democratic society».¹¹⁵ Ettersom vilkåret om legitimt formål er behandlet, siktes det med «rettmessighet» i denne sammenheng til de to øvrige vilkårene. I dette kapittelet skal det legges frem hvordan rettmessigheten av inngrep ved myndighetenes innhenting, lagring og behandling av åpent tilgjengelig informasjon skal vurderes. Deretter skal det vurderes om PSTs adgang etter forslag til politiregisterloven § 65 a er et rettmessig inngrep i EMK artikkel 8.

5.2 Rettmessighetsvurderingen i saker fra EMD om bulkinnsamling

Hovedtilnærmingen til EMD når de vurderer om myndighetenes tiltak er i tråd med menneskerettighetene i EMK er separate vurderinger av om inngrepet er i tråd med loven, ivaretar et legitimt formål og er nødvendig og forholdsmessig.¹¹⁶

I saker om overvåkning er det gjennomgående at EMD vurderer lovkravet og kravet om nødvendighet samlet.¹¹⁷ EMD har lagt til grunn at medlemsstatene «enjoy a fairly wide margin of appreciation» ved å velge hvilke tiltak som må til for å beskytte den nasjonale sikkerhet gjennom hemmelige overvåkningstiltak av myndighetene.¹¹⁸ Imidlertid knyttes det en fare for misbruk ved overvåkningssystemer foretatt av myndighetene. Til dette bemerker EMD at «the risk that a system of secret surveillance set up to protect national security may undermine or even destroy democracy under the cloak of defending it, the Court must be satisfied that there are adequate and effective guarantees against abuse.»¹¹⁹ Videre bemerkes det at vurderingene av lovkravet og kravet om nødvendighet er nært beslektet i disse tilfellene, som fordrer at de skal behandles i en samlet vurdering.

¹¹⁵ Jf. EMK artikkel 8 nr. 2.

¹¹⁶ Jf. ordlyden i EMK artikkel 8 nr. 2.

¹¹⁷ *Roman Zakharov mot Russland* [GC] 2015, no. 47143/06 avsnitt 232, *Szabó og Vissy mot Ungarn* [J] 2016, no. 37138/14 avsnitt 57-58, *Weber og Saravia mot Tyskland* [J] 2006, no. 54934/00 avsnitt 106, *Centrum för rättvisa* avsnitt 248 og 252-253, og *Big Brother Watch* avsnitt 334 og 338-339.

¹¹⁸ *Roman Zakharov mot Russland* [GC] 2015, no. 47143/06 avsnitt 232, *Szabó og Vissy mot Ungarn* [J] 2016, no. 37138/14 avsnitt 57, *Weber og Saravia mot Tyskland* [J] 2006, no. 54934/00 avsnitt 106, *Centrum för rättvisa* avsnitt 252, og *Big Brother Watch* avsnitt 338.

¹¹⁹ *Roman Zakharov mot Russland* [GC] 2015, no. 47143/06 avsnitt 232, *Szabó og Vissy mot Ungarn* [J] 2016, no. 37138/14 avsnitt 57, *Weber og Saravia mot Tyskland* [J] 2006, no. 54934/00 avsnitt 106, *Centrum för rättvisa* avsnitt 253, og *Big Brother Watch* avsnitt 339.

EMD legger vekt på om rettsgrunnlaget for inngrepet inneholder adekvate og effektive garantier mot misbruk. Det overordnede vurderingstemaet er likevel om inngrepet er nødvendig i et demokratisk samfunn, slik dette er formulert i EMK artikkel 8 nr. 2.¹²⁰ Således innebærer «in accordance with the law» at inngrepet må ha grunnlag i nasjonal lovgivning, og være «compatible with the rule of law».¹²¹ Det sistnevnte refererer til «quality of law» som innebærer at lovgrunnlaget må være tilstrekkelig tilgjengelig og forutsigbart.¹²² I saker om hemmelig overvåkning vil kravet til forutberegnelighet ha en annen dimensjon, ettersom de registrerte ofte ikke får vite at de er underlagt myndighetenes søkelys. Med forutberegnelighet vises det her til at lovgrunnlaget må med tilstrekkelig klarhet gi de utsatte adekvat beskyttelse mot vilkårlige inngrep.¹²³

EMD har ikke vurdert spørsmålet om rettmessigheten av innhenting, lagring og behandling av åpent tilgjengelig informasjon. EMD har imidlertid etablert en framgangsmåte i saker hvor myndighetene tillates å samle inn informasjon om borgerne, åpent eller skjult.¹²⁴ Ytterligere er det en fare for misbruk ved systemet om PSTs innhenting, lagring og behandling på grunn av hemmeligholdet. Dermed vil denne framgangsmåten følges i den videre analysen.

5.3 Rettssikkerhetsmekanismer i EMDs praksis

Rettssikkerhetsmekanismer er minimumsgarantier som må fremgå av hjemmelsgrunnlaget for å hindre maktmisbruk fra myndighetene.¹²⁵

I tidligere avgjørelser fra EMD i saker som har handlet om målrettet overvåkning, har domstolen utarbeidet seks krav.¹²⁶ EMD har lagt til grunn at disse kravene også gjelder i saker der innhenting var begrunnet i nasjonal sikkerhet.¹²⁷ I *Big Brother Watch* og *Centrum för rättvisa* var det behov for å tilpasse disse seks kravene når det gjaldt bulkinnstilling. EMD

¹²⁰ *Roman Zakharov mot Russland* [GC] 2015, no. 47143/06 avsnitt 236, *Szabó og Vissy mot Ungarn* [J] 2016, no. 37138/14 avsnitt 57, *Centrum för rättvisa* avsnitt 248, og *Big Brother Watch* avsnitt 334.

¹²¹ *Roman Zakharov mot Russland* [GC] 2015, no. 47143/06 avsnitt 228, *Szabó og Vissy mot Ungarn* [J] 2016, no. 37138/14 avsnitt 58, *Weber og Saravia mot Tyskland* [J] 2006, no. 54934/00 avsnitt 84, *Centrum för rättvisa* avsnitt 246, og *Big Brother Watch* avsnitt 332.

¹²² *Roman Zakharov mot Russland* [GC] 2015, no. 47143/06 avsnitt 228, *S. and Marper mot Storbritannia* [GC] 2008, nos. 30562/04 og 30566/04 avsnitt 95, *Centrum för rättvisa* avsnitt 246, og *Big Brother Watch* avsnitt 332.

¹²³ *Roman Zakharov mot Russland* [GC] 2015, no. 47143/06 avsnitt 51, *Weber og Saravia mot Tyskland* [J] 2006, no. 54934/00 avsnitt 94, *Centrum för rättvisa* avsnitt 247, og *Big Brother Watch* avsnitt 333.

¹²⁴ *Centrum för rättvisa* avsnitt 275 og *Big Brother Watch* avsnitt 361.

¹²⁵ Eksempelvis *Centrum för rättvisa* avsnitt 249 og *Big Brother Watch* avsnitt 335.

¹²⁶ Eksempelvis *Roman Zakharov mot Russland* [GC] 2015, no. 47143/06 avsnitt 231 og *Weber og Saravia mot Tyskland* [J] 2006, no. 54934/00 avsnitt 95.

¹²⁷ *Roman Zakharov mot Russland* [GC] 2015, no. 47143/06 avsnitt 231.

bemerket at den forutgående listen med rettssikkerhetsmekanismer var fra avgjørelser som er mer enn ti år gamle, og viste med dette til den teknologiske utviklingen.¹²⁸ Ytterligere at det er forskjell på overvåkning i form av henholdsvis målrettet innhenting og bulkinnsamling.¹²⁹ Herunder at ved bulkinnsamling er innsamlingen i utgangspunktet ikke rettet mot individer, men at det også kan foretas rettede søk.¹³⁰ Sammenholdt med behovet for hemmelighold er det en betydelig risiko for misbruk ved bulkinnsamlingssystemet.¹³¹ I begge kammeravgjørelsene ble staten felt.¹³² Domstolen fant at bulkinnsamlingssystemene ikke inneholdt tilstrekkelige «end-to-end safeguards» som sikret adekvate og effektive sikringstiltak mot vilkårlighet og misbruk.¹³³

EMD bemerket at ettersom inngrepet øker underveis i prosessen ved bulkinnsamling, er det behov for «end-to-end safeguards». Herunder at nødvendigheten og proporsjonaliteten må vurderes på ethvert trinn i prosessen. Med dette ble det fremhevet viktigheten av uavhengig autorisasjon før innhenting finner sted, og at gjennomføringen bør være underlagt tilsyn og etterfølgende vurderinger. EMD uttaler at dette er fundamentale sikkerhetstiltak som utgjør grunnlaget for enhver vurdering av bulkinnsamlingssystemer etter EMK artikkel 8.¹³⁴

På bakgrunn av dette formulerte EMD de følgende rettssikkerhetsmekanismer for bulkinnsamlingssystemer: (1) Grunnlaget for at bulkinnhenting kan tillates, (2) Hvilke omstendigheter som kan medføre innhenting av enkeltpersoners kommunikasjon, (3) Hvilke prosedyrer som gjelder for å gi autorisasjon til innhenting, (4) Hvilke prosedyrer som gjelder for seleksjon, analyse og bruk av innhentede data, (5) Hvilke forholdsregler som må tas dersom innhentede data skal overføres til andre, (6) Tidsbegrensninger for innhenting, lagring av innhentet data og omstendighetene som gjør at innhentet data må slettes, (7) Hvilke prosedyrer som gjelder for uavhengig tilsyn og kontroll, og deres kompetanse til å adressere manglende etterlevelse, og (8) Hvilke prosedyrer som gjelder for uavhengig

¹²⁸ *Centrum för rättvisa* avsnitt 255 og *Big Brother Watch* avsnitt 341.

¹²⁹ *Big Brother Watch* avsnitt 343.

¹³⁰ *Centrum för rättvisa* avsnitt 260 og *Big Brother Watch* avsnitt 346.

¹³¹ *Centrum för rättvisa* avsnitt 263 og *Big Brother Watch* avsnitt 349.

¹³² *Centrum för rättvisa* avsnitt 374 og *Big Brother Watch* avsnitt 427.

¹³³ *Centrum för rättvisa* avsnitt 373 og *Big Brother Watch* avsnitt 425.

¹³⁴ *Centrum för rättvisa* avsnitt 264 og *Big Brother Watch* avsnitt 350.

etterhåndskontroll, og hvilken kompetanse kontrollorganet har til å adressere manglende etterlevelse.¹³⁵ Samtidig ble det lagt til grunn at det måtte foretas en samlet vurdering.¹³⁶

Dermed er det en vurdering av om det nasjonale regelverket inneholder tilstrekkelige garantier mot misbruk og derav at systemet er underlagt «end-to-end safeguards». Herunder den faktiske gjennomføringen av systemet, kontroll og balanse ved maktutøvelsen, og kontroll ved misbruk.¹³⁷ Sammenfattet anerkjenner EMD at statene har en vid skjønnsmargin i tilfeller om ivaretagelse av nasjonal sikkerhet. Det må imidlertid stilles krav til metodene myndighetene velger som fremgangsmåte for å ivareta dette formålet. Ved å stille krav til en klar og forutberegnelig lovtekst skal det sikres at borgerne i tilstrekkelig grad er informert om hva myndighetene har adgang til å gjøre. Ved å ha uavhengig kontroll over prosessen sikres det at myndighetene underlegges kontroll og ikke misbruker adgangen til å innhente, lagre og behandle opplysninger. Uten en klarhet i hva PST kan gjøre eller en prosess som sørger for en uavhengig kontroll, er det en fare for myndighetsmisbruk. Poenget med vurderingen er at myndighetene skal, så langt det er mulig, ivareta enkeltpersoners rett til privatliv.

Rettsikkerhetsmekanismene som fremgår av avgjørelsene om bulkinnsamling, henholdsvis *Big Brother Watch* og *Centrum för rättvisa*, skal utgjøre «the cornerstone of any Article 8 compliant bulk interception regime».¹³⁸ Dette viser at kriteriene som er utarbeidet fra EMD ikke nødvendigvis kun skal anvendes når bulkinnsamlingen er benyttet i utenlandsetterretning, men bulkinnsamlingssystemer generelt. Som vist til må det foretas en helhetlig vurdering av momentene. Momentene er i seg selv generelt formulert som betyr at de kan anvendes på en rekke ulike saker hvor det innhentes informasjon om borgerne. Disse momentene vil danne utgangspunkt for den videre fremstillingen.

Følgelig skal det tas utgangspunkt i rettmessighetsvurderingen i *Big Brother Watch* og *Centrum för rättvisa*. Alle kravene må ikke være fullstendig oppfylt ettersom EMD legger opp til en samlet vurdering.¹³⁹ Den forskjellige graden av inngrep, særlig vedrørende innhenting av informasjon og hvilken informasjon det gjelder, vil hensyntas i den avsluttende og samlede vurderingen.

¹³⁵ *Centrum för rättvisa* avsnitt 275 og *Big Brother Watch* avsnitt 361.

¹³⁶ *Centrum för rättvisa* avsnitt 365 følgende og *Big Brother Watch* avsnitt 424 følgende.

¹³⁷ *Centrum för rättvisa* avsnitt 274 og *Big Brother Watch* avsnitt 360.

¹³⁸ *Centrum för rättvisa* avsnitt 264.

¹³⁹ *Centrum för rättvisa* avsnitt 365 følgende og *Big Brother Watch* avsnitt 424 følgende.

5.4 Er PSTs adgang til innhenting, lagring og behandling av åpent tilgjengelig informasjon et rettmessig inngrep i EMK artikkel 8?

5.4.1 Grunnlaget for at bulkinnhenting kan tillates

I dette kravet legger EMD at grunnlaget for bulkinnsamlingen må være tilstrekkelig klart utformet for å beskrive når bulkinnsamling kan gjennomføres.¹⁴⁰ Med grunnlaget siktes det ikke bare til hjemmelsteksten, men også begrunnelsen for hjemmelen som ofte finnes i formålet og forarbeider.¹⁴¹ Det må hensyntas at ulike trusler kan variere og endres over tid,¹⁴² som tilsier at det tillates at hjemmelen ikke angir presist hvilke tilfeller det skal være adgang til å samle inn opplysninger. EMD viser til at dersom grunnlaget for bulkinnsamling er vidt formulert er det større potensiale for misbruk.¹⁴³ Imidlertid fremheves det at selv om grunnlaget er formulert snevert, er det kun garanti mot misbruk dersom det inneholder tilstrekkelige sikringstiltak.¹⁴⁴ I *Big Brother Watch* fant EMD at grunnlaget var vidt formulert, men valgte å vurdere dette samlet med de øvrige vurderingskriteriene.¹⁴⁵ I *Centrum för rättvisa* kom EMD frem til at grunnlaget var klart formulert og begrunnet, ettersom det var klart avgrenset for å tillate nødvendig kontroll på autorisasjons- og operasjonsstadiet og etterfølgende kontroll.¹⁴⁶

Problemstillingen er om politiregisterloven ny § 65 a er tilstrekkelig klart utformet for når innhenting kan tillates.

Det fremgår ingen informasjon av politiregisterloven ny § 65 a eller den tilhørende forskriftsbestemmelsen politiregisterforskriften ny § 21-8¹⁴⁷ om selve innhenting. Det fremstår i høringsnotatet som om vilkåret for innhenting er det samme som behandlingen. Herunder at åpent tilgjengelig informasjon kan innhentes dersom det er «nødvendig for etterretningsvirksomheten», jf. forslag til politiregisterloven § 64 tredje ledd nytt nr. 6,¹⁴⁸ eller til «etterretningsformål», jf. forslag til politiregisterloven § 65 a første ledd. Det er klart at EMDs vilkår om at inngrepet må følge av lov er oppfylt dersom forslaget til

¹⁴⁰ *Centrum för rättvisa* avsnitt 285.

¹⁴¹ Se eksempelvis *Centrum för rättvisa* avsnitt 287 om «preparatory works».

¹⁴² *Centrum för rättvisa* avsnitt 285.

¹⁴³ *Big Brother Watch* avsnitt 370.

¹⁴⁴ *Big Brother Watch* avsnitt 370.

¹⁴⁵ *Big Brother Watch* avsnitt 371.

¹⁴⁶ *Centrum för rättvisa* avsnitt 288.

¹⁴⁷ Høringsnotatet punkt 7.3.

¹⁴⁸ Høringsnotatet punkt 7.2.

politiregisterloven ny § 65 a vedtas av Stortinget. Ytterligere er det uomtvistet at dersom politiregisterloven § 65 a vedtas at den er «adequately accessible» ettersom den da er lovfestet og tilgjengelig for allmenheten.

De krav som stilles til opplysningens kvalitet, jf. politiregisterloven § 6, og særlige kategorier av personopplysninger, jf. politiregisterloven § 7, omhandler behandlingen av opplysninger. Ved målrettet innhenting er det en forutsetning at denne informasjonen vil bli behandlet. Det kan dermed antas at det ikke har vært en problematikk knyttet til PSTs tidligere adgang til innhenting av opplysninger. Ved den foreslåtte adgangen i høringsnotatet vil PST kunne innhente betydelige mengder informasjon som skal lagres og behandles uten hensyn til personvern hensynene i §§ 6 og 7. Følgelig vil innhenting ha større konsekvenser for personvernet enn den tidligere adgangen. Det må dermed stilles krav til at innhenting må fremgå uttrykkelig av regelverket.

Etter EMDs praksis stilles det krav til hva som inngår i innhentingsadgangen.

Lovbestemmelsen, forskriftsbestemmelsen eller høringsnotatet for øvrig, inneholder ikke informasjon om hvordan innhenting skal foregå. Det er heller ikke klarlagt i forslaget hva som er utløsende årsaker for at PST kan innhente åpent tilgjengelig informasjon. Ettersom det ikke fremgår slike momenter av hjemmelsgrunnlaget, vil det være PST som avgjør når innhenting skal finne sted og i hvilken utstrekning. Etter EMDs praksis burde ordlyden i bestemmelsen, eller det tilhørende regelverk, være utformet på en måte som gjør at det må foretas en vurdering av vilkår før slik masseinnhenting tillates. Dermed er ikke forslag til politiregisterloven § 65 a, og regelverket for øvrig, tilstrekkelig utformet ut ifra EMDs praksis. Det må stilles vilkår til innhenting, slik at det er mulig å kontrollere at vilkårene blir overholdt. Imidlertid kan et bredt hjemmelsgrunnlag oppveies av andre garantier og sikkerhetsmekanismer som minimerer faren for misbruk. Derav vil dette tas med videre til den samlede vurderingen.

5.4.2 Hvilke omstendigheter som kan medføre innhenting av enkeltpersoners kommunikasjon

Dette kravet innebærer en vurdering av om det er tilstrekkelig klart og forutberegnelig i hvilke tilfeller individers kommunikasjon kan bli innhentet.¹⁴⁹ EMD bemerker at ved bulkinnsamling

¹⁴⁹ *Centrum för rättvisa* avsnitt 294 og *Big Brother Watch* avsnitt 376.

er hjemmelsgrunnlaget vidt utformet i hvilke tilfeller data kan innhentes.¹⁵⁰ I bulkinnsamlingsregimene i både *Centrum för rättvisa* og *Big Brother Watch* var formålet å innhente utenlandsk kommunikasjonsdata.¹⁵¹ Imidlertid var det på bakgrunn av den teknologiske innhentingens vanskelig å skille mellom innlands og utenlands data.¹⁵² I *Big Brother Watch* vurderte EMD om det hadde vært en forskjell om lovgrunnlaget var formulert mer nøyaktig.¹⁵³ Ettersom hverken avsender eller mottaker vet hvor eller kan kontrollere hvor den elektroniske kommunikasjonen går, ville ikke loven blitt mer forutberegnelig dersom den hadde blitt begrenset ytterligere.¹⁵⁴ I *Centrum för rättvisa* bemerket EMD at kommunikasjonsdata som hentes inn og ikke er til formålet, er mindre inngripende dersom det begrunnes at denne dataen ikke skal brukes til nærmere undersøkelse til etterretningsformål.¹⁵⁵ I begge avgjørelsene konkluderte EMD på dette punktet at lovgrunnlagene var tilstrekkelig forutberegnelige og klart utformet for i hvilke tilfeller data kan innhentes.¹⁵⁶

Problemstillingen er om forslag til politiregisterloven § 65 a er tilstrekkelig klart og forutberegnelig utformet for når det kan foretas innhenting av enkeltpersoners kommunikasjon eller personopplysninger.

Det må stilles krav til at hjemmelsgrunnlaget er tilstrekkelig spesifisert i hvilke tilfeller det kan innhentes informasjon fra individer. Dette har særlig betydning for forutberegneligheten. Selv om det ikke fremgår av høringsnotatet eller politiregisterloven ny § 65 a noe om hvordan innhentingens skal foregå, er informasjonen som skal innhentes «åpent tilgjengelig informasjon». Som vist til i inngrepsvurderingen er det en problematikk knyttet til inngrepsgraden av denne definisjonen.¹⁵⁷

Departementet har i høringsnotatet lagt til grunn hva som inngår i definisjonen. Det er informasjon som er allment tilgjengelig for offentligheten.¹⁵⁸ At det baseres på hvilken kontroll som utføres på nettstedet, herunder at åpent tilgjengelig informasjon omfatter

¹⁵⁰ *Centrum för rättvisa* avsnitt 289.

¹⁵¹ *Centrum för rättvisa* avsnitt 290 og *Big Brother Watch* avsnitt 374.

¹⁵² *Centrum för rättvisa* avsnitt 290 og *Big Brother Watch* avsnitt 375.

¹⁵³ *Big Brother Watch* avsnitt 376.

¹⁵⁴ *Big Brother Watch* avsnitt 376.

¹⁵⁵ *Centrum för rättvisa* avsnitt 292.

¹⁵⁶ *Centrum för rättvisa* avsnitt 294 og *Big Brother Watch* avsnitt 376.

¹⁵⁷ Se punkt 3.2.2.

¹⁵⁸ Høringsnotatet punkt 1.

nettsteder som eksempelvis krever opprettelse av abonnement eller bruker.¹⁵⁹ Ytterligere fremgår det en negativ avgrensning i politiregisterloven ny § 65 a første ledd at informasjonen ikke er «åpent tilgjengelig dersom tilgang krever forsering av passord eller lignende beskyttelsesmekanismer». Det er uklart hvor langt «nødvendig for etterretningsvirksomheten», jf. forslag til politiregisterloven § 64 tredje ledd nytt nr. 6, og ny § 65 a annet ledd nr. 1, rekker. Det kan stilles spørsmål ved hvor mange ledd ut man kan gå for at det fortsatt anses som nødvendig i forhold til formålet. Eksempelvis om det er nødvendig å kartlegge naboen til en høyreekstremist for å se om de har kontakt. Nødvendighetsvurderingen er skjønnsmessig, særlig når det er opp til PST å avgjøre. På denne måten kan det vanskelig være forutberegnelig for i hvilke tilfeller PST anser det som nødvendig til formålet å innhente informasjon fra åpne kilder.

I *Big Brother Watch* ble det vurdert om lovgrunnlaget kunne formuleres mer nøyaktig.¹⁶⁰ Det er klart at ordlyden i forslag til politiregisterloven § 65 a eller tilhørende forskriftsbestemmelse § 21-8 kunne blitt formulert på en måte som gjør innhentingsadgangen klar og forutberegnelig i større utstrekning. En meningsfull restriksjon er å legge avgrensninger til hvilken informasjon som kan innhentes. Eksempelvis kan det fremgå en avgrensning til bruk av ulike kategorier av selektorer. Herunder at søkebegrepene ikke direkte kan gå etter sensitive kategorier av personopplysninger, som for eksempel religiøs tilknytning og seksuell legning. Den foreslåtte ordlyden i politiregisterloven ny § 65 a, politiregisterforskriften § 21-8 og høringsnotatet for øvrig inneholder dermed ikke en tilstrekkelig klar og forutberegnelig definisjon på i hvilke tilfeller enkeltpersoners informasjon kan bli innhentet etter EMDs praksis.

5.4.3 Hvilke prosedyrer som gjelder for å gi autorisasjon til innhenting

Vurderingen er om det ligger til grunn tilstrekkelige rettssikkerhetsmekanismer som forhindrer misbruk eller uproporsjonale bulkinnsamlinger.¹⁶¹ Her vurderer EMD om bulkinnsamlingen blir autorisert av et uavhengig organ. Det kreves imidlertid ikke at det er en domstol.¹⁶² EMD legger til grunn at en vurdering av et uavhengig organ bør finne sted før bulkinnsamlingen starter når omfanget av innhenting legges til grunn.¹⁶³ Ytterligere har

¹⁵⁹ Høringsnotatet punkt 5.2.3.

¹⁶⁰ *Big Brother Watch* avsnitt 376.

¹⁶¹ *Centrum för rättvisa* avsnitt 302.

¹⁶² *Centrum för rättvisa* avsnitt 265.

¹⁶³ *Big Brother Watch* avsnitt 350.

EMD vurdert at etterfølgende endringer, etter den innledende fase av bulkinnsamlingen, burde hensyntas.¹⁶⁴ EMD vurderer det som mangelfullt dersom det ikke gis oversikt over kategorier av selektorer ved innhenting av informasjon.¹⁶⁵ Vurderingen beror på om det ligger til grunn et rammeverk for systemet som inneholder tilstrekkelige kontrollmekanismer ved innhenting av informasjon.

Problemstillingen er om det fremgår tilstrekkelige kontrollmekanismer ved PSTs innhenting av åpent tilgjengelig informasjon.

EOS-utvalgets kontroll skal omfatte blant annet PSTs «innhenting av informasjon», jf. EOS-kontrolloven § 6 annet ledd. Det fremgår av høringsnotatet at EOS-utvalget skal føre kontroll med behandlingen av informasjonen,¹⁶⁶ imidlertid er ikke spørsmålet om kontroll ved den innledende innhenting berørt. Dermed er det problematisk å vurdere hvilken kontroll som kan føres ved PSTs masseinnhenting av åpent tilgjengelig informasjon. Det er ikke belyst om, eller i hvilken utstrekning det skal tilrettelegges for at EOS-utvalget får innsyn i hvilke selektorer som brukes ved innhenting. Uansett vanskeliggjøres EOS-utvalgets kontroll ettersom vilkårene for PSTs innhentingsadgang er vidt formulert. Ettersom det ikke er vurdert ytterligere om kontroll ved innhenting i høringsnotatet, legges det til grunn at det ikke foreligger tilstrekkelige sikringstiltak ved PSTs tilgang til å innhente åpent tilgjengelig informasjon etter EMDs praksis.

5.4.4 Hvilke prosedyrer som gjelder for seleksjon, analyse og bruk av innhentede data

Ved dette momentet vurderer EMD systemet som følges ved utvelgelsen, undersøkelsen og bruken av det innhentede materialet. En generell uttalelse av EMD på dette punktet er at plikten til å føre logger og detaljert oversikt over ethvert trinn i prosessen vedrørende bulkinnsamlingssystemer, inkludert selektorene, må fremgå av lovgivningen.¹⁶⁷

I *Centrum för rättvisa* knyttet problematikken seg til at det var mangelfullt av svenske myndigheter å henvise til interne instruksjoner, og at det ikke fremgår uttrykkelig av loven. EMD kom imidlertid frem til at kravet var oppfylt ettersom loven inneholdt tilstrekkelige

¹⁶⁴ *Big Brother Watch* avsnitt 381 og 382.

¹⁶⁵ *Big Brother Watch* avsnitt 382 og 383.

¹⁶⁶ Høringsnotatet punkt 1.

¹⁶⁷ *Centrum för rättvisa* avsnitt 311.

sikkerhetstiltak mot misbruk. Herunder at det ble holdt tilsyn med alle aspekter av denne virksomheten i Sverige.¹⁶⁸ EMD la til grunn at svensk lovgivning inneholdt spesifikk beskyttelse for personlige data. Som at personlige data som ble behandlet måtte være adekvat og relevant til formålet, og kun personlige data som er nødvendig kunne bli behandlet. Alle rimelige midler skulle brukes til å rette, blokkere og slette personopplysninger som er uriktige eller ufullstendige i forhold til formålet.¹⁶⁹ Ytterligere var det et forbud i det svenske bulkinnsamlingssystemet mot å behandle personlige data kun på grunn av en persons rase eller etnisitet, politisk, religiøs eller filosofiske meninger, medlemskap i en fagforening, helse eller seksualliv.¹⁷⁰ Videre ble det lagt vekt på hvilke krav det stiltes til de som behandlet opplysningene. De ansatte som behandlet personopplysninger måtte være sikkerhetsgodkjent, underlagt taushetsplikt og forpliktet til å håndtere personopplysningene på en sikker måte, og kunne møte strafferettslige sanksjoner dersom de forvaltet opplysningene feil.¹⁷¹

I *Big Brother Watch* knyttet problematikken seg til at grunnlaget for hvilken informasjon som var gjenstand for nærmere undersøkelse var mangelfullt ettersom det var generelt utformet.¹⁷² EMD kom imidlertid frem til at loven allikevel var tilstrekkelig. Herunder at det stiltes krav om at den som analyserte innholdet måtte vurdere graden av inngrepet og hvordan inngrepet skulle minimeres. Analytikerens arbeid var for en definert tidsperiode, og dersom han skulle utvide tidsbruken måtte det en oppdatert begrunnelse til.¹⁷³ Det skulle bli gjennomført regelmessige kontroller for å sikre at informasjonen ble satt sammen på riktig måte. Det innsamlede materialet kunne bare undersøkes nærmere av autoriserte personer som hadde fått regelmessig obligatorisk opplæring ved bestemmelsene og kravene til nødvendighet og proporsjonalitet.¹⁷⁴ Den innhentede informasjonen kunne bare kopieres i den grad det var nødvendig for de autoriserte formålene. Kopiene skulle sikres og lagres på en sikker måte slik at det ikke var tilgjengelig for noen andre enn de autoriserte personene.¹⁷⁵ På bakgrunn av dette kom EMD frem til at systemet var tilstrekkelig forutberegnelig og hadde tilstrekkelige sikkerhetstiltak mot misbruk.¹⁷⁶

¹⁶⁸ *Centrum för rättvisa* avsnitt 311.

¹⁶⁹ *Centrum för rättvisa* avsnitt 312.

¹⁷⁰ *Centrum för rättvisa* avsnitt 314.

¹⁷¹ *Centrum för rättvisa* avsnitt 312.

¹⁷² *Big Brother Watch* avsnitt 386.

¹⁷³ *Big Brother Watch* avsnitt 388.

¹⁷⁴ *Big Brother Watch* avsnitt 389.

¹⁷⁵ *Big Brother Watch* avsnitt 390.

¹⁷⁶ *Big Brother Watch* avsnitt 391.

EMD la til grunn i *Centrum för rättvisa* at en viktig avgrensning på undersøkelsesstadiet er at analytikerne er forpliktet til å forkaste innhentet innenlandsk kommunikasjon umiddelbart etter at det er identifisert.¹⁷⁷ EMD la vekt på at til tross for at skillet mellom innlands og utlands kommunikasjon ikke var vanntett mot avskjæring ved den automatiske innhenting, måtte utelukkelsen av innlands kommunikasjon anses som en vesentlig begrensning av myndighetenes skjønn og et viktig sikkerhetstiltak mot misbruk, og derav som beskyttelse av enkeltpersoners rettigheter.¹⁷⁸ I *Big Brother Watch* var det også en avgrensning mot å bruke selektorer som hentet frem informasjon knyttet til nasjonale borgere.¹⁷⁹ Det er grunn til å bemerke at dette gjaldt en tjeneste som operer med utlandsetterretning, mens PST skal drive innenlandsetterretning. På generelt grunnlag får dette betydning for at loven må være utformet på en måte som legger opp til en tilstrekkelig og meningsfull restriksjon. Poenget er at myndighetene, så langt det er mulig, skal ivareta enkeltpersoners rett til privatliv og avgrense mot de tilfellene hvor det ikke er nødvendig å behandle informasjon som kan identifiseres med enkeltpersoner.

Sammenfattet må det ligge til grunn meningsfulle avgrensninger mot personopplysninger som ikke er av betydning til formålet. Ved menneskelig behandling av opplysningene må det stilles krav til de personene som gjennomfører behandlingen og får tilgang til denne. Det må fremgå av lovgivningen hvilken informasjon som kan behandles, hvem som kan behandle informasjonen og på hvilken måte informasjonen behandles. For å etterfølge dette må det foreligge sikringstiltak som sikrer at det ikke er rom for misbruk av myndighetene.

Det første spørsmålet er om norsk lovgivning i tilstrekkelig grad gir uttrykk for hvilken informasjon som kan behandles av PST og hvordan informasjonen kan brukes av PST.

Etter forslag til politiregisterloven § 63 tredje ledd ny nr. 6 vil PST ha en hjemmel til å behandle opplysninger som er «nødvendig for etterretningsvirksomheten». Etter politiregisterloven ny § 65 a annet ledd punkt 1 til 3 kan opplysningene behandles og brukes til formål om etterretningsvirksomhet, opprettelse av eller i bruk av forebyggende sak, eller etterforskning. Nødvendighetskravet er nærmere definert i politiregisterloven § 5 og politiregisterforskrift § 21-2. Imidlertid er det etter bestemmelsene betydelige mengder

¹⁷⁷ *Centrum för rättvisa* avsnitt 307.

¹⁷⁸ *Centrum för rättvisa* avsnitt 308.

¹⁷⁹ *Big Brother Watch* avsnitt 384.

tilfeller hvor informasjon om enkeltpersoner kan bli behandlet. Det legger i stor grad opp til PSTs skjønn å avgjøre hvilken informasjon som kan behandles. Det må bemerkes at ved bestemmelsene som allerede er lovfestet, er det ikke tatt i betraktning at behandlingen som følger av politiregisterloven ny § 65 a er unntatt lovens §§ 6 og 7. Dette åpner for en videre adgang til behandling og bruk av opplysninger.

Behandlingen og bruken av den innhentede informasjonen overlapper alle de tre formålene PST skal ivareta. PST har dermed en vid adgang til behandling og bruk. Følgelig kan det med utgangspunkt i forslag til politiregisterloven § 65 a vanskelig avklares hvilken informasjon som er gjenstand for nærmere undersøkelse, og er dermed generell i sin utforming. Det er heller ikke lagt frem i høringsnotatet hvordan søk skal foregå med selektorer for behandling av materialet. Det kunne med fordel vært presisert hvilken informasjon som kan bli gjenstand for nærmere undersøkelse. Imidlertid forelå den samme problematikken om et generelt utformet lovgrunnlag i både *Centrum för rättvisa* og *Big Brother Watch*. EMD vurderte om dette kravet likevel kunne anses oppfylt dersom det forelå tilstrekkelige sikringstiltak som ivaretar enkeltpersoners rett til privatliv.

Videre er problemstillingen om lovgivningen, så langt det er mulig, ivaretar enkeltpersoners rett til privatliv med sikringstiltak ved PSTs behandling av den innhentede informasjonen.

Det første underspørsmålet er om PSTs behandling av den innhentede informasjonen i tilstrekkelig grad oppfyller kravene til personer som foretar nærmere undersøkelser etter EMDs praksis. Etter forslag til politiregisterforskriften § 21-8 første ledd annet punktum¹⁸⁰ kan kun personer som har fått «særskilt bemyndigelse» få tilgang til opplysningene. I høringsnotatet er det fremhevet at opplysningene som er sperret skal begrenses til så få personer som mulig og at kun personer som har fått særskilt bemyndigelse skal behandle opplysningene.¹⁸¹ Det fremgår ikke hva som inngår i «særskilt bemyndigelse» i høringsnotatet.

Politiregisterforskriften § 8-4 omhandler kvalifikasjonskrav og bemyndigelse. Forskriften gjelder for når PST behandler opplysninger etter politiregisterloven § 64 og hjemler i annen lovgivning, jf. politiregisterforskriften § 20-2, jf. § 20-1. Ettersom forskriftsbestemmelsen til

¹⁸⁰ Høringsnotatet punkt 7.3.

¹⁸¹ Høringsnotatet punkt 3.2.

politiregisterloven ny § 65 a, ny § 21-8, er i samme forskrift, legges det til grunn at de samme reglene gjelder for særskilt bemyndigelse, jf. systembetraktninger. Kun personer som har gjennomgått opplæring kan gis tilgang til opplysninger, og det skal legges til grunn nærmere bestemte retningslinjer om kvalifikasjonskrav, jf. politiregisterforskriften § 8-4 første ledd. Det følger av annet ledd annet punktum at særskilt bemyndigelse kun skal gis til «kvalifiserte personer som har gjennomgått opplæring». Ved utøvelse av offentlig myndighet kan en straffes for tjenestefeil etter straffeloven §§ 171 og 172, og brudd på eventuell taushetsplikt etter straffeloven § 209. Med dette anses kravene etter EMDs praksis til personer som foretar nærmere undersøkelser som oppfylt.

Således er det neste underspørsmålet om lovgivningen inneholder tilstrekkelig beskyttelse for personlige data. Herunder at alle rimelige midler skal brukes til å rette, blokkere og slette personopplysninger som er uriktige eller ufullstendige til formålet. Departementet legger frem i høringsnotatet at mye av informasjonen som blir innhentet er av «mindre interesse for PSTs oppgaveløsning».¹⁸² Videre fremgår det at opplysningene skal sperres¹⁸³ og holdes atskilt fra PSTs øvrige system.¹⁸⁴ Dette innebærer at kun personer med særskilt bemyndigelse kan foreta søk i opplysningene.

Imidlertid er det knyttet usikkerhet til PSTs system vedrørende sperring. I årsmelding fra EOS-utvalget fra eksempelvis 2017 er det bemerket en problematikk med sperrefunksjonen. Herunder at det ikke er gjennomført en tilfredsstillende løsning for sperring av opplysninger.¹⁸⁵ Dette gjaldt også med hensyn til sletting av opplysninger. Dette har tilsynelatende ikke blitt bedre i senere tid.¹⁸⁶

Det er foreslått en lengste slettefrist på 15 år. Det fremgår av høringsnotatet at PST må slette informasjon som ikke inneholder opplysninger av etterretningsmessig verdi eller ikke er nødvendig til etterretningsformål. Det gjelder imidlertid kun om tjenesten blir «klar over» dette forhold.¹⁸⁷ Denne slettefunksjonen er ikke foreslått fastsatt i lovbestemmelsen eller den tilhørende forskriftsbestemmelsen. Det vil være opp til PSTs skjønn å vurdere når denne

¹⁸² Høringsnotatet punkt 5.2.2.

¹⁸³ Høringsnotatet punkt 7.2, politiregisterloven ny § 65 a annet ledd.

¹⁸⁴ Høringsnotatet punkt 7.3, politiregisterforskriften ny § 21-8 første ledd.

¹⁸⁵ Årsmelding fra Stortingets kontrollutvalg for etterretnings-, overvåkings- og sikkerhetstjeneste (EOS-utvalget) for 2017, dokument 7:1 (2018-2019) punkt 4 og punkt 5.5.

¹⁸⁶ EOS-utvalgets høringsuttalelse 17.12.2021 til Justis- og beredskapsdepartementet punkt 2.5 og 2.6.

¹⁸⁷ Høringsnotatet punkt 5.2.8.

informasjonen skal slettes utenfor lengstefristen, og kan dermed vanskelig kontrolleres. Ytterligere er det gjort unntak fra politiregisterloven § 7 om behandling av særlige kategorier av personopplysninger. Dette er viktige personvern hensyn, og i eksempelvis *Centrum för rättvisa* var det et viktig moment i vurderingen at disse hensynene var ivare tatt ved behandlingen av informasjon.¹⁸⁸ Sammenholdt med problematikken knyttet til sikringstiltakene, henholdsvis ved sperring og sletting, foreligger det ikke tilstrekkelig beskyttelse for personlige data etter EMDs praksis.

Det neste underspørsmålet er om det er tilstrekkelig lagt opp til tilsyn med alle aspekter av PSTs behandling av den innhentede informasjonen etter EMDs praksis. Det følger av høringsnotatet at PSTs bruk av opplysningene skal kunne spores for å avdekke urettmessig bruk, og at EOS-utvalget kan føre kontroll.¹⁸⁹ Imidlertid er det usikkerhet knyttet til hvilken informasjon EOS-utvalget vil få ved bruk av teknologiske verktøy. EOS-utvalget uttaler i sin høringsuttalelse at det er nødvendig at PST tilrettelegger systemene med kontrollmuligheter for at det skal kunne utføres kontroll.¹⁹⁰ Det følger av høringsnotatet at EOS-utvalget skal kontrollere PSTs bruk av sperret informasjon og derav hvem som har tilgang til opplysningene.¹⁹¹ Det fremgår ingen ytterligere informasjon om slik tilrettelegging i høringsnotatet. Problematikken knyttet til innsyn i selektorer eller andre tekniske virkemidler er ikke belyst. Heller ikke vedrørende sperring og sletting av opplysninger. Følgelig må det legges til grunn at det ikke er tilstrekkelig tilrettelagt for kontroll på det nåværende tidspunkt. Dermed er det ikke tilstrekkelig lagt opp til tilsyn ved alle aspekter ved PSTs behandling av informasjonen som det kreves etter EMDs praksis.

Sammenfattet er hjemmelsgrunnlaget for PSTs behandling av informasjon generelt utformet. Ytterligere er ikke regelverket utformet på en måte som tilstrekkelig ivaretar enkeltpersoners rett til privatlivet ved PSTs behandling av informasjonen etter politiregisterloven ny § 65 a. Forslaget oppfyller dermed ikke kravene som følger av EMDs praksis på dette punktet.

¹⁸⁸ Jf. ovenfor, *Centrum för rättvisa* avsnitt 312.

¹⁸⁹ Høringsnotatet punkt 1.

¹⁹⁰ EOS-utvalgets høringsuttalelse 17.12.2021 til Justis- og beredskapsdepartementet punkt 2.7.

¹⁹¹ Høringsnotatet punkt 6.

5.4.5 Hvilke forholdsregler som må tas dersom innhentede data deles med andre

Dette er et krav om å vurdere nødvendighet og proporsjonalitet for de mulige innvirkningene på rettighetene etter EMK artikkel 8 ved deling til andre.¹⁹² Dette må fremgå klart av lovgrunnlaget, og kan ikke være for generelt utformet.¹⁹³ Problematikken ved dette kravet i *Big Brother Watch* og *Centrum för rättvisa* knyttet seg i hovedsak til overføringen av den innhentede informasjonen til utenlandske sikkerhetstjenester.¹⁹⁴ I *Big Brother Watch* var lovgrunnlaget for delingen tilstrekkelig klart og inneholdt tilstrekkelige garantier mot misbruk.¹⁹⁵ EMD la vekt på at det engelske systemet inneholdt krav om å forsikre at mottakeren hadde sikkerhetstiltak om sikker lagring og bruk av informasjonen, og som hindret misbruk.¹⁹⁶ Samt ødeleggelse av data når det ikke lengre var nødvendig til formålet.¹⁹⁷

Vedrørende deling av data til nasjonale organer er det krav om at rettssikkerhetsmekanismene også gjelder for de andre organene som mottar informasjonen.¹⁹⁸ Beskyttelse av informasjonen må innebære «end-to-end safeguards» og må dermed også gjøres gjeldende for andre som mottar informasjonen. Det må vurderes om det er risiko for misbruk, og om det ligger til grunn tilstrekkelige sikringstiltak for å unngå misbruk også ved nasjonal deling.

Det fremgår av høringsnotatet at informasjonen som sperres ikke vil kunne utleveres til andre.¹⁹⁹ Dette følger ikke av ordlyden i forslaget til politiregisterloven § 65 a eller den tilhørende forskriftsbestemmelsen politiregisterforskriften § 21-8. Imidlertid kan det fortolkes at informasjonen ikke skal utleveres til andre ettersom de sperrede opplysningene bare kan brukes til de nevnte formål i ny § 65 a annet ledd punkt 1 til 3. Imidlertid skal PST samarbeide enten nasjonalt²⁰⁰, med eksempelvis politiet, eller med utenlandske myndigheter²⁰¹, som eksempelvis politimyndigheter og sikkerhets- og etterretningstjenester. Dermed burde det fremgå klart av lovgrunnlaget om og eventuelt når opplysningene kan deles med andre aktører. Dersom dette ved vedtakelse kun fremgår av forarbeidene, vil det uansett

¹⁹² *Centrum för rättvisa* avsnitt 323.

¹⁹³ *Centrum för rättvisa* avsnitt 322.

¹⁹⁴ *Centrum för rättvisa* avsnitt 320 følgende, og *Big Brother Watch* avsnitt 395 følgende.

¹⁹⁵ *Big Brother Watch* avsnitt 399.

¹⁹⁶ *Big Brother Watch* avsnitt 395.

¹⁹⁷ *Big Brother Watch* avsnitt 396.

¹⁹⁸ *Centrum för rättvisa* avsnitt 317 og *Big Brother Watch* avsnitt 392-394.

¹⁹⁹ Høringsnotatet punkt 5.2.6 premiss 9.

²⁰⁰ Jf. Instruks for Politiets sikkerhetstjeneste § 10.

²⁰¹ Jf. Instruks for Politiets sikkerhetstjeneste § 11.

ligge til grunn lov som gir PST adgang til å utlevere opplysningene.²⁰² Som følge av denne uklarheten skal PSTs adgang til utlevering av informasjon adresseres tydeligere.

Problemstillingen er om det er tilstrekkelig ivaretatt at det skal foreligge sikringstiltak ved deling til andre.

Reglene om utlevering av opplysninger som fremgår av politiregisterloven kapittel 5 og 6 og politiregisterforskrift del 3 gjelder for PST, jf. politiregisterforskrift § 21-7 første ledd. Det følger av politiregisterloven § 19 at PST kan utlevere opplysninger dersom reglene om taushetsplikt i politiregisterloven kapittel 6, vilkårene i § 8 annet ledd og § 20 er oppfylt. Det spesifiseres ikke hvem informasjonen kan deles til.

Etter politiregisterloven § 21 kan tjenestemenn i politiet og påtalemyndigheten gis tilgang ved direkte søk til PSTs opplysninger «i den utstrekning det er tjenestemessig behov, og det er til formål som omfattes av denne loven». Politiregisterlovens regler gjelder også for politiet og påtalemyndighetene, jf. § 3. Således er politiet og påtalemyndigheten regulert av de samme reglene som PST ved behandling av opplysninger. Imidlertid er politiet og påtalemyndighetene ikke unntatt §§ 6 og 7 ved behandling av opplysninger. Dermed er politiet og påtalemyndigheten underlagt strengere reguleringer enn PST ved behandling av den innhentede informasjonen. Det er stilt ytterligere krav til informasjonssikkerhet og internkontroll i §§ 15 og 16. Ytterligere skal bruken av opplysninger kunne spores, og informasjonen om bruk av system skal registreres og lagres, jf. § 17. Databehandlere i politiet og påtalemyndighetene kan heller ikke behandle personopplysninger som ikke følger av skriftlig avtale eller instruks, jf. § 18. Ettersom politiet eller påtalemyndighetene gis tilgang til opplysningene ved direkte søk etter skriftlig avtale, tilsier det at informasjonen ikke nødvendigvis vil overføres til deres databaser. Sammenfattet kan det ved deling til politiet og påtalemyndigheten anses som at kravet er oppfylt vedrørende deling av opplysninger.

Det fremgår av politiregisterloven § 22 at PSTs opplysninger kan utleveres til utenlandske myndigheter. Før opplysningene blir delt til utenlandske myndigheter skal det foretas en nødvendighetsvurdering, jf. politiregisterforskriften § 9-9 tredje ledd første punktum. Herunder at det blant annet skal «legges vekt på hvordan opplysningene vil bli brukt eller behandlet i mottakerlandet», jf. tredje ledd annet punktum. Ved deling av opplysninger til

²⁰² Se politiregisterloven kapittel 5, jf. politiregisterforskriften § 21-7 første ledd.

land som «ikke har gjennomført direktiv (EU) 2016/680» gjelder det ytterligere regler for å ivareta personvernet, jf. fjerde ledd. Med dette er kravene etter EMDs praksis ved deling til internasjonale myndigheter og deres bruk og behandling av opplysningene ved deling tilstrekkelig ivaretatt.

Problematikken knyttet til deling av den innhentede informasjonen er ikke belyst i høringsnotatet. Det kan med fordel fremheves hvorvidt det er aktuelt med annen deling enn det som fremgår av politiregisterloven. Dette er for å kunne vurdere at all deling av de innhentede opplysningene oppfyller kravene som fremgår av EMDs praksis. Vedrørende deling til andre, slik det fremgår av politiregisterloven, er hensynet til å ivareta sikringstiltak ved PSTs deling av informasjon tilstrekkelig ivaretatt etter kravene i EMDs praksis.

5.4.6 Tidsbegrensninger for innhenting, lagring av innhentet data og omstendighetene som gjør at innhentet data må slettes

EMD viser til at varigheten av innhenting er opp til nasjonale myndigheter å avgjøre. Det må imidlertid foreligge tilstrekkelige sikkerhetstiltak. Herunder at det fremgår klart av lovgivningen hvor lenge innhenting kan vare, hvilke vilkår som må ligge til grunn for å fornye innhenting og under hvilke omstendigheter det ikke kan tillates innhenting.²⁰³

Det stilles krav til lagring av det innhentede materialet og når data må slettes eller destrueres. EMD legger til grunn at et minimumskrav er at det må stilles «legal requirement» til å slette innhentet data som ikke lengre har betydning til formålet det er innhentet til.²⁰⁴ Dette gjelder for data som kan innvirke på rettighetene beskyttet av EMK artikkel 8, herunder både personopplysninger og korrespondanse.²⁰⁵ EMD legger til grunn at det må foreligge tilstrekkelig informasjon om hvordan nødvendigheten til å fortsette lagringen av dataen eller destrueringen av personopplysninger vurderes, om den ubehandlede informasjonen lagres i maksimaltiden, og om nødvendigheten av fortsatt lagring blir jevnlig gjennomgått. Dersom det ikke fremgår tilstrekkelig av lovgrunnet, vanskeliggjør det vurderingen av lagring og sletting av den innhentede informasjonen. Vedrørende dette punkt, vurderer EMD dette nærmere under kravet om etterfølgende kontroll.²⁰⁶ Til tross for mangelfullt grunnlag, konkluderer EMD i *Centrum för rättvisa* om lagring og sletting av informasjonen med at

²⁰³ *Centrum för rättvisa* avsnitt 331.

²⁰⁴ *Centrum för rättvisa* avsnitt 342.

²⁰⁵ *Centrum för rättvisa* avsnitt 342.

²⁰⁶ *Centrum för rättvisa* avsnitt 343.

kravet er oppfylt.²⁰⁷ I *Big Brother Watch* fant EMD at lagringen og slettingen av det innhentede materialet i praksis var tilstrekkelig for å oppfylle kravene på dette punktet. Imidlertid var det en svakhet med systemet at det ikke var lovfestet.²⁰⁸

Problemstillingen er om forslag til politiregisterloven § 65 a oppfyller kravene til varighet av innhenting, og lagring og sletting av innhentet data.

Det første underspørsmålet er om politiregisterloven ny § 65 a oppfyller kravene til varighet ved innhenting av informasjon. Som vist til ovenfor er hjemmelen til innhenting vidt formulert.²⁰⁹ Det er dermed etter PSTs skjønn å avgjøre i hvilke tilfeller innhenting skal skje og hvor lenge innhenting skal vare. Dette er ikke i tråd med EMDs uttalelser, hvor det kreves at det fremgår uttrykkelig av regelverket.

Det andre underspørsmålet er om PSTs adgang til lagring av åpent tilgjengelig informasjon oppfyller kravene til lagring og sletting. Det stilles krav til at PST sletter informasjon som ikke er nødvendig for å ivareta nasjonal sikkerhet. Som vist til tidligere, foreligger det ingen krav om at PST skal slette informasjon ut over den maksimale lagringstiden etter politiregisterloven ny § 65 a eller tilhørende regelverk.²¹⁰ Dette er opp til PSTs skjønn. Dette er ikke i tråd med EMDs krav om at det skal fremgå uttrykkelig av regelverket. Til tross for mangelfullt grunnlag kan det likevel godkjennes dersom kravene til etterfølgende kontroll er oppfylt.

EMD kommer ikke uttrykkelig med uttalelser om lengden av lagret informasjon. Imidlertid må det som følge av kravet til nødvendighet og forholdsmessighet tas i betraktning hvor lang den maksimale lagringstiden er i relasjon til kravet om sletting av informasjonen. Det kan legges til grunn at en lagringstid på 15 år er lang. Lagringstiden er begrunnet i at PST skal kartlegge og følge trender over tid. Det kan imidlertid stilles spørsmål ved hvilken etterretningsverdi opplysninger har etter 15 år. Eller om en kan stole på så gammel informasjon, særlig sett i sammenheng med at opplysningene ikke skal rettes eller være nøyaktige. Dersom informasjonen skal være for å kartlegge trender, er det nærliggende at PST skal utarbeide rapporter basert på informasjonen. Det må legges til grunn at PST vil forvalte

²⁰⁷ *Centrum för rättvisa* avsnitt 344.

²⁰⁸ *Big Brother Watch* avsnitt 405.

²⁰⁹ Se punkt 5.4.1.

²¹⁰ Se punkt 5.4.4.

denne informasjonen fortløpende. Det er dermed vanskelig å forestille seg hvilken etterretningsverdi 15 år gammel informasjon vil ha. Når det gjelder etterforskning vil 15 år gammel informasjon, som ikke nødvendigvis inneholder korrekt informasjon, ikke alltid ha en verdi til dette formålet. Heller ikke til forebyggende sak. Et alternativ er at det foretas en gjennomgang etter noen år for å slette informasjon som ikke er nødvendig til formålet. Sammenfattet foreligger det ikke tilstrekkelige sikringstiltak vedrørende sletting og lagring av informasjonen etter EMDs praksis.

5.4.7 Hvilke prosedyrer som gjelder for uavhengig tilsyn og kontroll, og deres kompetanse til å adressere manglende etterlevelse

Vurderingen beror på om kontrollorganet er en fungerende sikkerhetsmekanisme mot misbruk på alle stadier i bulkinnstillingen.²¹¹ EMD så på hvilke institusjoner som overholder tilsyn etter lovsystemet.²¹² Således om denne hadde en rolle som uavhengig kontrollmekanisme ut i fra dens organisering.²¹³ Videre måtte tilsynsorganet ha fullmakter til å vurdere etterlevelsen av de formelle kravene i lovgivningen, samt vurdere forholdsmessigheten av eventuelle inngrep i de individuelle rettigheter.²¹⁴ Herunder ble det lagt vekt på at undersøkelsene av det uavhengige organet innebærer nærmere undersøkelser av hvilke selektorer som ble brukt av etterretningstjenestene.²¹⁵ EMD tok også i betraktning hvordan kontrollene ble utført i praksis, herunder at det i praksis måtte fungere som en effektiv kontroll.²¹⁶ Ytterligere stiltes det krav til at det uavhengige kontrollorganet kunne treffe avgjørelser som hadde rettslig og bindende virkning.²¹⁷

Problemstillingen er om EOS-utvalget fungerer som en tilstrekkelig effektiv og uavhengig kontrollmekanisme ved tilsyn av PST.

Det første underspørsmålet er om EOS-utvalget er uavhengig i dens organisering. Etter politiregisterloven § 68 første ledd skal EOS-utvalget utøve tilsyn med PSTs behandling av opplysninger. EOS-utvalget er valgt av Stortinget og skal kontrollere etterretnings-, overvåkings- og sikkerhetstjenestene, jf. EOS-kontrollloven § 1 første ledd. Innenfor rammene

²¹¹ *Centrum för rättvisa* avsnitt 353.

²¹² *Centrum för rättvisa* avsnitt 345 og *Big Brother Watch* avsnitt 406.

²¹³ *Centrum för rättvisa* avsnitt 346 og *Big Brother Watch* avsnitt 407.

²¹⁴ *Centrum för rättvisa* avsnitt 347-348, og *Big Brother Watch* avsnitt 408.

²¹⁵ *Centrum för rättvisa* avsnitt 348 og *Big Brother Watch* avsnitt 412.

²¹⁶ *Centrum för rättvisa* avsnitt 351 og *Big Brother Watch* avsnitt 410-411.

²¹⁷ *Centrum för rättvisa* avsnitt 350.

av EOS-kontrollloven skal EOS-utvalget utføre sitt verv «selvstendig og uavhengig av Stortinget», jf. EOS-kontrollloven § 1 femte ledd. På denne måten er EOS-utvalget tilstrekkelig uavhengig i dens organisering.

Det andre underspørsmålet er om EOS-utvalgets oppgaver er tilstrekkelige til å foreta en vurdering av PSTs virksomhet. EOS-utvalget skal gjennomføre kontroll og regelmessige inspeksjoner av PST, jf. § 5 første ledd. Det stilles krav til minste antall årlige inspeksjoner EOS-utvalget skal foreta av PST, og ut over dette skal inspeksjonene gjennomføres etter behov, jf. EOS-kontrollloven § 7. Utvalget skal av eget tiltak ta opp alle saker og forhold som det ut ifra «formålet er riktig å behandle, og særlig slike som har vært gjenstand for kritikk», jf. § 5 tredje ledd første punktum. Herunder er «forhold» regelverk, direktiver og praksis, jf. tredje ledd annet punktum. Stortinget kan pålegge EOS-utvalget å foreta nærmere definerte undersøkelser, jf. § 1 femte ledd annet punktum. Utvalget skal kontrollere at PST i samsvar med lovens formål etter § 2, jf. § 6 første ledd. Herunder blant annet kontrollere at det ikke benyttes midler som er mer inngripende enn nødvendig etter forholdene, klarlegge og forebygge at enkeltpersoners rettigheter krenkes, og at PST respekterer menneskerettighetene i utførelsen av oppgavene sine, jf. § 2 første ledd punkt 1.

Utvalgets kontroll omfatter PSTs tekniske virksomhet, vedrørende «overvåkning og innhenting av informasjon og behandling av personopplysninger», jf. § 6 annet ledd. Utvalget kan foreta beslutninger om innsyn og utstrekning av kontrollen, som er bindende for forvaltningen, jf. § 8 fjerde ledd. På anmodning fra utvalget plikter enhver som tjenestegjør i PST å legge frem informasjon som kan ha betydning for kontrollen, jf. § 8 annet ledd. Dermed innebærer EOS-utvalgets kontroll av PST at de skal vurdere at oppgavene opptres i tråd med regelverket og at inngrep er nødvendige til formålet. Følgelig oppfylder EOS-utvalgets oppgaver kravene etter EMDs praksis.

Det neste underspørsmålet er om EOS-utvalget holder tilstrekkelig effektiv kontroll med PST. Det fremgår av EOS-kontrollloven § 14 første ledd at utvalget «har rett til å uttale sin mening om forhold som omfattes av kontrollområdet». Ordlyden av «rett til å uttale sin mening» tilsier at det ikke er uttalelser med bindende virkning. Videre følger det av § 14 at utvalget kan «påpeke», jf. annet ledd, «foreslå forbedringer», jf. tredje ledd, eller komme med «uttalelser som gir oppfordring», jf. siste ledd. Derav fremgår det ikke av bestemmelsen eller loven for øvrig at EOS-utvalget har myndighet til å treffe bindende beslutninger. I årsmeldingene til Stortinget kan utvalget gjøre Stortinget oppmerksom på forhold eller

problemstillinger som er aktuelle, og anbefale lovendringer, jf. EOS-kontrolloven § 17 annet og tredje ledd.²¹⁸ Eksempelvis at utvalget bemerker problematikken knyttet til PSTs sperring og sletting av opplysninger til Stortinget.

Utvalget har imidlertid ikke instruksjons- eller vedtaksmyndighet overfor PST. Utvalget kan fremme uttalelser om forhold det undersøker eller gi anbefalinger. Dersom EOS-utvalget eksempelvis avdekker at PST behandler informasjon som ikke er til formålet, vil det ikke kunne stoppe behandlingen med bindende virkning. EOS-utvalgets kompetanse er dermed begrenset og stikkprøvebasert. Dette oppfyller ikke kravet til at kontrollorganet skal treffe avgjørelser som har rettslig og bindende virkning etter EMDs praksis.

5.4.8 Hvilke prosedyrer som gjelder for uavhengig etterhåndskontroll, og hvilken kompetanse kontrollorganet har til å adressere manglende etterlevelse

På grunn av hemmelighold i slike operasjoner kan ikke etterretningen underrette enkeltpersoner om at deres kommunikasjon er overvåket.²¹⁹ EMD fremholder imidlertid at dette må oppveies ved effektive rettsmidler for enkeltpersoner som mistenker at deres kommunikasjon er overvåket.²²⁰ I *Centrum för rättvisa* kom EMD frem til at dette kravet ikke var oppfylt. Det ble lagt vekt på at kontrollorganet ikke hadde tilstrekkelig med informasjon til å vurdere hvilke selektorer, eller kategorier av selektorer, som ble lagt til grunn for innhenting av data, eller vedrørende ødeleggelse av det innhentede materialet. Dette ble vektlagt fordi det forsterket usikkerheten for de berørte individene om hvorvidt vilkårlighet eller misbruk kunne forekomme.²²¹

Problemstillingen er om systemet ved PSTs innhenting, lagring og behandling av åpent tilgjengelig informasjon inneholder tilstrekkelige sikringstiltak for etterfølgende kontroll.

Det første underspørsmålet er om enkeltpersoner har tilstrekkelige rettsmidler gjennom kontrollorganet, herunder adgang til å klage og at klagen kan medføre en reell rettsvirkning. Ettersom EOS-utvalget kontrollerer PSTs virksomhet, kan enkeltpersoner og organisasjoner klage til utvalget. EOS-utvalget avgjør om klagen skal behandles ved nærmere undersøkelser, jf. EOS-kontrolloven § 5 annet ledd. Etter politiregisterloven § 68 annet ledd første punktum

²¹⁸ Se punkt 5.4.4.

²¹⁹ *Centrum för rättvisa* avsnitt 354.

²²⁰ *Centrum för rättvisa* avsnitt 355.

²²¹ *Centrum för rättvisa* avsnitt 364.

skal EOS-utvalget kontrollere at opplysningene om den registrerte er behandlet i samsvar med loven, dersom det følger av begjæring fra den registrerte. Dermed er det en tilstrekkelig klageadgang til utvalget som blir fulgt opp.

EOS-utvalgets uttalelser til klagere skal være «så fullstendige som mulig uten at det gis graderte opplysninger», jf. EOS-kontrolloven § 15 første ledd første punktum. Imidlertid fremgår det av bestemmelsens første ledd tredje punktum at vedrørende klager mot PST om overvåkmessig virksomhet «skal det bare uttales om klagen har gitt grunn til kritikk eller ikke». Dersom utvalget mener at klageren burde få en mer utfyllende begrunnelse, skal dette følge med som et forslag til PST, jf. første ledd siste punktum. En eventuell klage til EOS-utvalget om PSTs virksomhet kan innebære «kritikk eller meningsytring» fra utvalget, jf. § 15 annet ledd. På denne måten innebærer dette den samme problematikken som ved kravet ovenfor.²²² Herunder at utvalget har en reell adgang til å prøve PSTs virksomhet, men utfallet av kritikken ikke har reell virkning. Utvalget kan rette kritikk eller meningsytring til PST ved en klage, men det innebærer ingen rettslig eller bindende virkning for PST. Følgelig har ikke enkeltpersoner tilstrekkelige rettsmidler gjennom EOS-utvalget.

Det neste underspørsmålet er om EOS-utvalget kan holde tilstrekkelig kontroll med hvilke selektorer som brukes av PST. EOS-utvalget har etter forslaget ikke tilstrekkelig innsyn i selektorer, særlig knyttet til innhenting hvor det ikke er tilrettelagt for kontroll. Ytterligere er det problematikk knyttet til sletting og sperring av den innhentede informasjonen. Dette forsterker usikkerhet for den enkelte om vilkårlighet og misbruk.

Det må foreligge sikkerhetstiltak som tilstrekkelig overholder en etterfølgende kontroll av at individers rettigheter etter EMK artikkel 8 har blitt ivaretatt. Det kan stilles spørsmål ved om et slikt kontrolltiltak kan være at enkeltpersoner kan kreve at informasjon om dem som er uriktig eller publisert av andre kan bli søkt fjernet fra PSTs databaser, som deretter leder til en plikt til å undersøke og vurdere å fjerne dette innholdet. Imidlertid fremgår det ingen slik klageadgang, og det er heller ikke vurdert i høringsnotatet. I tillegg fremgår det av tvisteloven²²³ § 22-1 (1) at det ikke kan føres bevis om «noe som holdes hemmelig av hensyn til rikets sikkerhet». Dersom eksempelvis enkeltpersoner skal saksøke Staten ved PST for

²²² Se punkt 5.4.7.

²²³ Lov 17. juni 2005 nr. 90 om mekling og rettergang i sivile tvister (tvisteloven).

ulovlig innhenting av opplysninger, så gjelder det et forbud mot å føre bevis av opplysningene.

Sammenholdt med at klageadgangen til EOS-utvalget ikke har rettslig bindende virkning, inneholder ikke systemet tilstrekkelige sikringstiltak for etterfølgende kontroll etter kravet i EMDs praksis.

5.4.9 Den samlede vurderingen og konklusjon

Avslutningsvis vurderer EMD de fremlagte kravene samlet, herunder er det en vurdering av om systemet for bulkinnhenting inneholder tilstrekkelige «end-to-end» sikringsmekanismer. Dermed er det en avveining av hvilke tiltak som er oppfylt og ikke.²²⁴ I det følgende skal det foretas den samme vurderingen som etter EMDs praksis for å komme frem til om PSTs adgang til innhenting, lagring og behandling av åpent tilgjengelig informasjon etter forslag til politiregisterloven § 65 a utgjør et rettmessig inngrep i EMK artikkel 8. Innledningsvis skal det legges til grunn hvordan de ulike kravene skal vektlegges i denne vurderingen.

Det er uklart hvordan innhenting av åpent tilgjengelig informasjon skal vurderes etter EMK artikkel 8. I inngrepsvurderingen ble det lagt til grunn at det er mindre inngripende å innhente åpent tilgjengelig informasjon enn lukket kommunikasjon, som i kammeravgjørelsene fra EMD.²²⁵ I denne samlede vurderingen vil dermed kravene om innhenting, herunder grunnlaget for at bulkinnhenting kan tillates, hvilke omstendigheter som kan medføre innhenting av enkeltpersoners kommunikasjon, og hvilke prosedyrer som gjelder for å gi autorisasjon til innhenting, ikke få like stor betydning. Innhenting utgjør imidlertid et inngrep. EMD har lagt til grunn at det har betydning for proporsjonaliteten dersom tiltak utføres mot egne borgere. Det ble fremlagt i *Big Brother Watch* at innlands kommunikasjon også ble innhentet i relasjon til bulkinnhenting. EMD bemerket at myndighetene kan bruke mindre inngripende metoder mot egne borgere.²²⁶ Dette taler for at innhenting av informasjon fra åpne kilder likevel skal inngå i den samlede vurderingen. Følgelig kan svakheter ved innhenting ikke anses å ha avgjørende vekt, men vil virke som momenter i denne vurderingen.

²²⁴ Se *Centrum för rättvisa* avsnitt 365 følgende og *Big Brother Watch* avsnitt 424 følgende.

²²⁵ Punkt 3.2.3.

²²⁶ *Big Brother Watch* avsnitt 375.

Det er den videre behandlingen av informasjonen som gjør at forslaget mer inngripende enn det departementet legger til grunn i høringsnotatet. På samme måte som i *Big Brother Watch* og *Centrum för rättvisa* er systemet etter politiregisterloven ny § 65 a mer inngripende etter hvert når informasjonen lagres over lengre tid og blir utsatt for behandling og videre bruk. Det er denne behandlingen som medfører at det stilles høye krav til rettssikkerhetsmekanismer. Derav har de øvrige kravene som ikke direkte er knyttet til innhenting, like avgjørende betydning i den samlede vurderingen som i EMDs avgjørelser om bulkinnsamlingssystemer.

Problemstillingen er om PSTs adgang til innhenting, lagring og behandling av åpent tilgjengelig informasjon etter forslag til politiregisterloven § 65 a inneholder «end-to-end safeguards» og derav utgjør et rettmessig inngrep i EMK artikkel 8.

På den ene siden er det flere forhold vedrørende systemet for PSTs innhenting, lagring og behandling av åpent tilgjengelig informasjon som er i tråd med EMDs krav til bulkinnsamlingssystemer. Departementet har i høringsnotatet fremhevet viktigheten av sikringstiltak for å beskytte informasjonen. Eksempelvis ved å sperre informasjonen, og kravene som stilles til de autoriserte personene som behandler informasjonen nærmere. Ved deling til andre organer er det tilstrekkelige vurderinger vedrørende nødvendighet og at mottakeren også innehar sikringsmekanismer for å ivareta informasjonen. Ytterligere har EOS-utvalget som kontrollorgan adgang til å vurdere hele PSTs virksomhet. Utvalget er også et uavhengig organ og foretar uavhengige vurderinger av virksomheten. Følgelig foreligger det gunstige løsninger vedrørende PSTs bulkinnsamlingssystem.

På den annen side foreligger det svakheter ved systemet. Det fremgår ikke klart av forslag til ordlyd av politiregisterloven § 65 a eller systemet for øvrig når innhenting kan tillates. Heller fremgår det ikke hvor lenge innhenting kan forekomme. Hjemmelsgrunnlaget er vidt formulert for i hvilke tilfeller PST kan behandle informasjonen. I høringsnotatet er det ikke lagt frem hvordan søk skal foregå, med selektorer, når materialet er innsamlet. Eksempelvis kunne det med fordel vært avgrenset mot å innstille selektorene mot særlige kategorier av personopplysninger ved videre behandling, som «homofil» eller «Jehovas vitne». Det fremgår ingen vilkår i lovteksten utenom formålsbegrensningene. Lengstefristen for lagring av materialet er lang, 15 år, og det er usikkerheter knyttet til sperrefunksjonen som sikringstiltak. Det fremgår ikke av lovsystemet når informasjon burde slettes ut over lengstefristen, herunder om det ikke er til formålet.

Videre har EMD vektlagt rollen til et uavhengig kontrollorgan og deres kompetanse. EOS-utvalget som kontrollorgan har ikke kompetanse til å treffe avgjørelser som har rettslig eller bindende virkning overfor PST. Dette påvirker også at det ikke er en tilstrekkelig etterfølgende kontroll og effektive rettsmidler for enkeltpersoner. EOS-utvalgets kontroll burde vært adressert, men i høringsnotatet er ikke denne problematikken fremhevet. Det er dermed ikke i tråd med EMDs strenge krav til uavhengig kontroll. Heller tas det ikke hensyn til at masseinnsamling av informasjon mot egne borgere kan anses mer inngripende enn innsamling fra utlandet i høringsnotatet. Det er klart at innhenting, lagring og behandling av åpent tilgjengelig informasjon er nødvendig for PSTs oppdrag. Imidlertid må det foreligge tilstrekkelige sikringsmekanismer etter inngrepsgraden.

Selv om systemet inneholder flere sikringstiltak som er i tråd med EMDs praksis, er det flere forhold som ikke er belyst av departementet i høringsnotatet. Eksempelvis at EOS-utvalget ikke fører reell kontroll, om enkeltpersoners klageadgang får rettslige virkninger, og at enkelte deler ikke fremgår uttrykkelig av lovgrunnlaget, som krav til sletting ut over den maksimale lagringstiden. Ved å ikke vurdere ytterligere sikringstiltak som fremgår av EMDs praksis, viser det til at tiltaket ikke er holdt til det som er «necessary in a democratic society» etter EMK artikkel 8. Av særlig avgjørende betydning har det at det foreligger en lang lagringstid uten en tilstrekkelig begrunnelse til formålet og uten krav om sletting som fremgår av loven, og at systemet ikke innehar en reell kontrollfunksjon. Dersom systemet ikke innehar slike sikringstiltak, åpner det for vilkårlighet og misbruk. Sammenfattet inneholder ikke forslaget «end-to-end safeguards» som det kreves etter EMDs praksis.

Konklusjonen er at forslaget om PSTs adgang til innhenting, lagring og behandling av åpent tilgjengelig informasjon etter politiregisterloven § 65 a ikke er et rettmessig inngrep i EMK artikkel 8.

6 Avsluttende refleksjoner

Det er fundamentalt at PST følger med i trusselbildet og avdekker eksempelvis terrorplanlegging på internett.²²⁷ Det eksisterer imidlertid stater i dag der myndighetene fullstendig overvåker borgerne. Disse samfunnene har lite kriminalitet, og hvis noe, avdekkes det umiddelbart.²²⁸ Disse statene bruker overvåkning som et middel for å kontrollere borgerne, og har på denne måten ivaretatt sin rolle som beskytter. Hvorvidt dette er demokratiske stater, kan diskuteres.

Retten til privatliv er en nødvendig rettighet for å opprettholde et demokratisk samfunn, ettersom det innebærer at enhver har rett til å utfolde seg selv og sine meninger. Ved den nære sammenhengen til ytringsfriheten kan restriksjoner innebære en nedkjølende effekt på individers ytringer.²²⁹ Det er vanskelig å finne en riktig balanse mellom statens konstitusjonelle plikt til å beskytte borgerne mot kriminalitet, og til å beskytte borgernes rettigheter. Begge er avgjørende for å opprettholde et demokratisk samfunn. Spørsmålene som må stilles er om løsningene samsvarer med våre demokratiske rettsprinsipper og om disse får et ønskelig utfall.

I høringsnotatet fremstår det som om departementet har undervurdert inngrepsgraden av PSTs adgang til innhenting, lagring og behandling av åpent tilgjengelig informasjon i EMK artikkel 8.²³⁰ Det kan stilles spørsmål ved om tiltak som går ut over enkeltpersoners privatliv burde opplyses i større grad til befolkningen. Det må i alle tilfeller hensyntas hvilke innvirkninger et slikt tiltak vil ha på samfunnet for øvrig, og at inngrepet forholdes til det som er strengt nødvendig. Retten til privatliv blir utfordret ved den uunngåelige og kontinuerlige teknologiske utviklingen. Med dagens teknologiske verktøy kan myndighetene, teknisk sett, foreta en fullstendig overvåkning av borgerne. Dersom grensen til retten til privatliv stadig blir innskrenket, kan det medføre at rettigheten til slutt ikke eksisterer lengre. Hvor vi legger oss på spekteret mellom myndighetenes rolle som beskytter på den ene siden og enkeltpersoners rett til privatliv på den annen, har betydning for morgendagens Norge.

²²⁷ Se punkt 4.

²²⁸ Se eksempelvis Greg Walton, *China's golden shield: corporations and the development of surveillance technology in the People's Republic of China*, International Centre for Human Rights and Democratic Development 2001, side 5.

²²⁹ Se punkt 2.

²³⁰ Se punkt 3.

Referanseliste

Norske lover

Kongeriket Norges Grunnlov, Lov 17. mai 1814

Lov 3. februar 1995 nr. 7 om kontroll med etterretnings-, overvåkings- og sikkerhetstjenestene (EOS-kontrolloven)

Lov 4. august 1995 nr. 53 om politiet (politiloven)

Lov 21. mai 1999 nr. 30 om styrking av menneskerettighetenes stilling i norsk rett (menneskerettsloven – mrl.)

Lov 20. mai 2005 nr. 28 om straff (straffeloven – strl.)

Lov 17. juni 2005 nr. 90 om mekling og rettergang i sivile tvister (tvisteloven)

Lov 28. mai 2010 nr. 16 om behandling av opplysninger i politiet og påtalemyndigheten (politiregisterloven)

Norske forskrifter, instruksjer og kongelige resolusjoner

Instruks 19. august 2005 nr. 920 for Politiets sikkerhetstjeneste

Forskrift 20. september 2013 nr. 1097 om behandling av opplysninger i politiet og påtalemyndigheten (politiregisterforskriften)

Lovforarbeider og offentlige utredninger

NOU 2004: 6 Mellom effektivitet og personvern: Politimetoder i forebyggende øyemed

NOU 2009: 15 Skjult informasjon – åpen kontroll, Metodekontrollutvalgets evaluering av lovgivningen om politiets bruk av skjulte tvangsmidler og behandling av informasjon i straffesaker

Meld. St. 21 (2012–2013) Terrorberedskap — Oppfølging av NOU 2012: 14 Rapport fra 22. juli-kommisjonen

Høring om endringer i politiloven og politiregisterloven mv. PSTs etterretningsoppdrag og behandling av åpent tilgjengelig informasjon, Justis- og beredskapsdepartementet, 7. oktober 2021

Andre stortingsvedtak og stortingsdokumenter

Årsmelding fra Stortingets kontrollutvalg for etterretnings-, overvåkings- og sikkerhetstjeneste (EOS-utvalget) for 2017, dokument 7:1 (2018-2019), tilgjengelig på: https://eos-utvalget.no/wp-content/uploads/2019/05/2017_eos_a_rsmelding_net-1.pdf

Høyesterettsavgjørelser

Rt. 2000 s. 996 P (Bøhler)

Rt. 2005 s. 833 A

Rt. 2008 s. 1409 S

Rt. 2015 s. 93 A (Maria)

Rt. 2015 s. 155 A (Rwanda)

HR-2016-2554-P (Holship)

HR-2020-2372-A

Avgjørelser fra underinstanser

RG-2012-1153 (Oslo tingrett)

TAHER-2020-5113 (Asker og Bærum tingrett)

Internasjonale konvensjoner

Convention for the Protection of Human Rights and Fundamental Freedoms, Roma, 4. november 1950 (Den europeiske menneskerettighetskonvensjonen – EMK)

Vienna Convention on the Law of Treaties, Wien, 23. mai 1969 (Wien-konvensjonen)

Avgjørelser fra EMD

Golder mot Storbritannia	<i>Golder mot Storbritannia</i> [P], ECHR:1975:0221JUD000445170
Tyrer mot Storbritannia	<i>Tyrer mot Storbritannia</i> [J], ECHR:1978:0425JUD000585672
Klass og andre mot Tyskland	<i>Klass og andre mot Tyskland</i> [P], ECHR:1978:0906JUD000502971
Silver og andre mot Storbritannia	<i>Silver og andre mot Storbritannia</i> [J], ECHR:1983:0325JUD000594772
Leander mot Sverige	<i>Leander mot Sverige</i> [J], ECHR:1987:0326JUD000924881
Amann mot Sveits	<i>Amann mot Sveits</i> [J], ECHR:2000:0216JUD002779895
Rotaru mot Romania	<i>Rotaru mot Romania</i> [GC], ECHR:2000:0504JUD002834195
P.G. og J.H. mot Storbritannia	<i>P.G. og J.H. mot Storbritannia</i> [J], ECHR:2001:0925JUD004478798
Weber og Saravia mot Tyskland	<i>Weber og Saravia mot Tyskland</i> [J], ECHR:2006:0629DEC005493400
Association for European Integration and Human Rights og Ekimdzhiev mot Bulgaria	<i>Association for European Integration and Human Rights og Ekimdzhiev mot Bulgaria</i> [J], ECHR:2007:0628JUD006254000
S. and Marper mot Storbritannia	<i>S. and Marper mot Storbritannia</i> [GC], ECHR:2008:1204JUD003056204
Gillan and Quinton mot Storbritannia	<i>Gillan and Quinton mot Storbritannia</i> [J], ECHR:2010:0112JUD000415805
Ciubotaru mot Moldova	<i>Ciubotaru mot Moldova</i> [J], ECHR:2010:0427JUD002713804

Jehovah's Witnesses of Moscow og andre mot Russland	<i>Jehovah's Witnesses of Moscow og andre mot Russland</i> [J], ECHR:2010:0610JUD000030202
Uzun mot Tyskland	<i>Uzun mot Tyskland</i> [J], ECHR:2010:0902JUD003562305
Roman Zakharov mot Russland	<i>Roman Zakharov mot Russland</i> [GC], ECHR:2015:1204JUD004714306
Szabó og Vissy mot Ungarn	<i>Szabó og Vissy mot Ungarn</i> [J], ECHR:2016:0112JUD003713814
Mockutė mot Litauen	<i>Mockutė mot Litauen</i> [J], ECHR:2018:0227JUD006649009
Catt mot Storbritannia	<i>Catt mot Storbritannia</i> [J], ECHR:2019:0124JUD004351415
Centrum för rättvisa mot Sverige	<i>Centrum för rättvisa mot Sverige</i> [GC], ECHR:2021:0525JUD003525208
Big Brother Watch og andre mot Storbritannia	<i>Big Brother Watch og andre mot Storbritannia</i> [GC], ECHR:2021:0525JUD005817013

EU- og EØS rettsakter

Europaparlaments- og rådsdirektiv (EU) 2016/680 av 27. april 2016 om beskyttelse av fysiske personer ved behandling av personopplysninger for å forebygge, etterforske, avdekke eller straffeforfølge lovbrudd eller gjennomføring av straffereaksjoner, og om fri utveksling av slike opplysninger og opphevelse av rådets rammebeslutning 2008/977/JIS

Juridisk litteratur

Aall, Jørgen, *Rettsstat og menneskerettigheter*, 5. utgave, Fagbokforlaget 2018.

Skoghøy, Jens Edvin A., *Rett og rettsanvendelse*, Universitetsforlaget 2018.

Settem, Ola Johan, «Subsidiaritetsprinsippet og skjønnsmarginen i EMK-retten» *Jussens Venner*, vol. 51, Utg. 3, 30. juni 2016, pp. 119-141.

Mestad, Ola «Rettens kilder og anvendelse» i Alf Petter Høgberg (red.) og Jørn Øyrehagen Sunde (Red.), *Juridisk metode og tenkemåte*, Universitetsforlaget 2019.

Høringsuttalelser

Advokatforeningens høringsuttalelse til Justis- og beredskapsdepartementet av 03.01.2022, tilgjengelig på: <https://www.regjeringen.no/no/dokumenter/horing-endringer-i-politiloven-og-politiregisterloven-mv.-psts-etterretningsoppdrag-og-behandling-av-apent-tilgjengelig-informasjon.pdf/id2874615/?uid=3ce356d5-c579-43e0-a044-34f901eb8d2c> (lest 10.01.2022)

Datatilsynets høringsuttalelse til Justis- og beredskapsdepartementet av 05.01.2022, tilgjengelig på: <https://www.regjeringen.no/no/dokumenter/horing-endringer-i-politiloven-og-politiregisterloven-mv.-psts-etterretningsoppdrag-og-behandling-av-apent-tilgjengelig-informasjon.pdf/id2874615/?uid=c8fe24d0-69d4-436d-9ac8-921c920ebafa> (lest 10.01.2022)

EOS-utvalgets høringsuttalelse til Justis- og beredskapsdepartementet av 17.12.2021, tilgjengelig på: <https://www.regjeringen.no/no/dokumenter/horing-endringer-i-politiloven-og-politiregisterloven-mv.-psts-etterretningsoppdrag-og-behandling-av-apent-tilgjengelig-informasjon.pdf/id2874615/?uid=7a31c030-56a8-4a4b-8730-d54b6af7adf8> (lest 10.01.2022)

Norges institusjon for menneskerettigheters (NIM) høringsuttalelse til Justis- og beredskapsdepartementet av 07.01.2022, tilgjengelig på: <https://www.regjeringen.no/no/dokumenter/horing-endringer-i-politiloven-og-politiregisterloven-mv.-psts-etterretningsoppdrag-og-behandling-av-apent-tilgjengelig-informasjon.pdf/id2874615/?uid=97ea9f12-f0d4-4e90-a5b7-53f7d0c84764> (lest 10.01.2022)

Politiets sikkerhetstjenestes høringsuttalelse til Justis- og beredskapsdepartementet av 06.01.2022, tilgjengelig på: https://www.regjeringen.no/contentassets/797ff4cd55e6432d80ccd14be2d91807/annen-offentlig-etat/politiets-sikkerhetstjeneste.pdf?uid=Politiets_sikkerhetstjeneste (lest 09.02.2022)

Andre kilder

Chancellor, S., De Choudhury, M. Methods in predictive techniques for mental health status on social media: a critical review. *npj Digit. Med.* 3, 43 (2020), <https://doi.org/10.1038/s41746-020-0233-7> (lest 17.02.2022).

Datatilsynets hjemmesider, 05.01.2022, tilgjengelig på:

[https://www.datatilsynet.no/aktuelt/aktuelle-nyheter-2022/horing-om-pst-og-behandling-av-
apent-tilgjengelig-informasjon/](https://www.datatilsynet.no/aktuelt/aktuelle-nyheter-2022/horing-om-pst-og-behandling-av-
apent-tilgjengelig-informasjon/) (lest 27.01.2022)

Eirik Rossen, «IT» i Store norske leksikon, 6. november 2019, <https://snl.no/IT> (lest 10.03.2022).

Letvik, Tore og Tuva Bønke Grønning, «Hacking og datalekkasjer utgjør en stor trussel for personvernet», Juristen, 16. mars 2022 [https://juristen.no/nyheter/2022/02/--hacking-og-
datalekkasjer-utgjor-en-stor-trussel-personvernet](https://juristen.no/nyheter/2022/02/--hacking-og-
datalekkasjer-utgjor-en-stor-trussel-personvernet) (lest 05.04.2022).

Leuner, John, A Replication Study: Machine Learning Models Are Capable of Predicting Sexual Orientation From Facial Images (2019), <https://arxiv.org/abs/1902.10739> (lest 17.02.2022)

Nasjonal trusselvurdering 2021, PST, tilgjengelig på:

[https://www.pst.no/globalassets/artikler/trusselvurderinger/nasjonal-trusselvurdering-
2021/ntv_2021_final_web_1802-1.pdf](https://www.pst.no/globalassets/artikler/trusselvurderinger/nasjonal-trusselvurdering-
2021/ntv_2021_final_web_1802-1.pdf) (lest 02.02.2022)

Nasjonal trusselvurdering 2022, PST, tilgjengelig på:

<https://www.pst.no/globalassets/ntv/2022/nasjonal-trusselvurdering-2022-pa-norsk.pdf> (lest 02.02.2022)

PSTs hjemmesider: <https://www.pst.no/alle-artikler/artikler/dette-gjor-vi/> (lest 15.03.2022)

Regjeringens hjemmesider: [https://www.regjeringen.no/no/tema/statlig-forvaltning/ikt-
politikk/digitaliseringen-i-offentlig-sektor/id2340245/](https://www.regjeringen.no/no/tema/statlig-forvaltning/ikt-
politikk/digitaliseringen-i-offentlig-sektor/id2340245/) (lest. 23.02.2022)

Skriftlig spørsmål fra Guri Melby (V) til forsvarsministeren:

[https://www.stortinget.no/no/Saker-og-publikasjoner/Sporsmal/Skriftlige-sporsmal-og-
svar/Skriftlig-
sporsmal/?qid=86975&fbclid=IwAR1gwEuST2d6eLJbuHZBY6sO_JOICvTq1BSfrWg0hKm
V6KopgAS4nQy-iH0](https://www.stortinget.no/no/Saker-og-publikasjoner/Sporsmal/Skriftlige-sporsmal-og-
svar/Skriftlig-
sporsmal/?qid=86975&fbclid=IwAR1gwEuST2d6eLJbuHZBY6sO_JOICvTq1BSfrWg0hKm
V6KopgAS4nQy-iH0) (lest 09.02.2022)

Sunde, Inger Marie (Red.), «Forebygging av radikalisering og voldelig ekstremisme på internett», Rapport fra Politihøgskolen, 2013, tilgjengelig på:

https://www.regjeringen.no/contentassets/a52f793994fc474cbde714586dfc0762/rapport_forebygging-rad-eks.pdf (lest 21.03.2022)

Walton, Greg, *China's golden shield: corporations and the development of surveillance technology in the People's Republic of China*, International Centre for Human Rights and Democratic Development 2001. Tilgjengelig i PDF-format på:

<https://publications.gc.ca/collections/Collection/E84-7-2001E.pdf>

