Norges institusjon for menneskerettigheter

Justis- og beredskapsdepartementet
post@jd.dep.no

Deres referanse: 21/4559
Vår referanse: 2021/171
Dato: 07/01/2022

Høringsuttalelse - Endringer i politiloven og politiregisterloven mv. – PSTs etterretningsoppdrag og behandling av åpent tilgjengelig informasjon

1. Innledning

Vi viser til Justis- og beredskapsdepartementets høringsbrev av 7. oktober 2021 om forslag til endringer i politiloven og politiregisterloven mv. – PSTs etterretningsoppdrag og behandling av åpent tilgjengelig informasjon.

Norges institusjon for menneskerettigheter (NIM) har som hovedoppgave å fremme og beskytte menneskerettighetene i tråd med Grunnloven, menneskerettsloven og den øvrige lovgivning, internasjonale traktater og folkeretten for øvrig. Vi skal bidra til å styrke gjennomføringen av menneskerettighetene, særlig ved å gi råd og fremme anbefalinger til Stortinget, regjeringen, Sametinget og andre. Høringsuttalelser er et sentralt virkemiddel i dette arbeidet. I utgangspunktet er det ikke nødvendigvis NIMs oppgave å uttale seg om hensiktsmessigheten eller prioriteringen av virkemidler for å oppfylle menneskerettslige forpliktelser.

Slik vi forstår høringsnotatet består lovforslaget av to hovedelementer. Det ene gjelder lovfestingen av PSTs etterretningsmandat. Det andre gjelder adgangen til å behandle åpent tilgjengelig informasjon. NIM vil hovedsakelig komme med innspill til sistnevnte.

2. Departementets forslag og forholdet til menneskerettighetene

Forslaget om bruk av åpne kilder berører to viktige interesser, som i enkelte tilfeller kan stå i motsetning til hverandre. På den ene siden står statens plikt til å sikre egne borgere, herunder gjennom bekjempelse av alvorlig kriminalitet, terrorbekjempelse, og å beskytte grunnleggende nasjonale interesser. Staten har en plikt til å sikre innbyggernes liv og helse etter blant annet Den europeiske menneskerettskonvensjon (EMK) artikkel 2. Plikten til å forebygge og bekjempe terror følger også eksplisitt av flere internasjonale forpliktelser.[1] NIM anerkjenner at staten derfor har behov for verktøy som gjør den i stand til å oppfylle sin plikt til å sikre disse rettighetene og forebygge alvorlige trusler mot befolkningen. Det understrekes imidlertid at staten ikke har noen

[1] Se for eksempel Europarådets konvensjon om forebygging av terrorisme (ETS nr. 196).

plikt til å innføre bestemte systemer for overvåkning av borgerne. Hvilke tiltak som kan iverksettes for å sikre nasjonale interesser, forebygge terror og liknende lovbrudd må balanseres mot menneskerettighetene på den annen side, herunder retten til privatliv, personvernet og ytringsfriheten.

I høringsnotatet foreslås en ny bestemmelse i politiregisterloven som åpner for at PST kan lagre, systematisere og analysere store mengder åpent tilgjengelig informasjon til etterretningsformål. Forslaget vil åpne opp for generell innsamling og bruk av informasjon om norske borgere som vil ramme bredt, også personer helt uten interesse for PST, og vil gi PST anledning til å systematisere store mengder informasjon om samtlige borgere.

Selv om forslaget handler om innsamling av åpne kilder, vurderer NIM det slik at aktiviteten har betydelige likhetstrekk med skjult overvåking. Hvis forslaget vedtas må borgerne i fremtiden ta høyde for at det som publiseres på sosiale medier eller andre steder på internett, vil kunne bli gjenstand for analyser hos PST. Informasjonen er på den ene siden åpen ved at den enkelte ofte har foretatt den konkrete publiseringen uten noe bevisst ønske om eller behov for å skjule denne for andre. På den annen side vil ikke den enkelte være klar over hva som er samlet inn av PST, hvilke områder på internett PST laster ned informasjon fra, eller hvordan opplysningene kan brukes og sammenstilles. Effektene både for samfunnet og den enkelte minner derfor om skjult overvåkning. Dette har etter vårt syn stor betydning for hvilke rettssikkerhetsmekanismer som bør ledsage forslaget. Særlig er *omfanget* av den foreslåtte innsamlingen iøynefallende. At informasjonen er *åpen* er derfor ikke tilstrekkelig begrunnelse for å unnta forslaget fra rettssikkerhetsmekanismene som normalt kreves for etterretningsinnsamling for å vedta forslaget slik det nå foreligger. Vi kommer nærmere tilbake til dette nedenfor under pkt. 4.

Lovforslaget om innsamling av åpent tilgjengelig informasjon på de måter som foreslås i høringsnotatet kan utgjøre et stort inngrep i borgernes *privatliv og personvern*. Videre vil forslaget berøre *ytringsfriheten*, særlig i form av en nedkjølende effekt. Ytringsfriheten er avgjørende for et fungerende demokrati, og forslaget har flere klare sider til dette. NIM mener forslaget i sin nåværende form er svært omfattende, lite forutsigbart for borgeren, og at det må innføres ytterligere rettssikkerhetsmekanismer før adgangen til innsamling og bruk av slik informasjon kan innføres.

NIMs vurderinger og anbefalinger kan oppsummeres slik:

- NIM mener at flere sentrale problemstillinger og momenter ikke er tilstrekkelig berørt i høringsnotatet. NIM savner en bredere diskusjon om PSTs behov for å lagre så store mengder opplysninger, og avveiningen mot de sentrale menneskerettighetene dette berører. NIM mener forslaget er mer inngripende

enn departementet legger til grunn. Det bør derfor begrunnes mer inngående hvorvidt behandlingen er nødvendig i så stor utstrekning som foreslått.

- Det er ikke drøftet hvilken overføringsverdi EMDs praksis om bulkinnsamlingssystemer eller annen EMD-praksis kan få for forslaget. Det er heller ikke drøftet hvorvidt forskjellen mellom innsamling av informasjon fra utenlandske aktører og innsamling av informasjon fra egne borgere påvirker inngrepsgraden.
- Det fremgår ikke av høringsnotatet hva slags automatiske analyseverktøy som kan benyttes og hvordan disse skal innrettes.
- NIM etterlyser en grundigere vurdering av hvordan forslaget vil kunne virke nedkjølende på individers ønske om å ytre seg, særlig på nett, og hvorvidt forslaget vil påvirke samfunnet og demokratiet mer overordnet.
- NIM mener at den vide innsamlingsadgangen, lange lagringstiden, vide rammer for bruk, kombinert med bruken av automatiserte analyseverktøy tilsier at forslaget må møtes med strengere regler for lagring og andre rettssikkerhetsgarantier.
- Etter NIMs oppfatning vil forslaget ikke være forholdsmessig slik det nå foreligger i dag, og kan derfor ikke vedtas i en slik form.

3. Retten til privatliv

3.1. EMK artikkel 8 og Grunnloven § 102

Det følger av Grunnloven § 102 at enhver har rett til respekt for sitt privatliv og familieliv, sitt hjem og sin kommunikasjon. Tilsvarende følger det av EMK artikkel 8 at enhver har rett til respekt for sitt privatliv og familieliv, sitt hjem og sin korrespondanse.

Det er ingen tvil om at retten til privatliv beskytter mot den typen forslag som det her er tale om. Den europeiske menneskerettsdomstol (EMD) har i flere tilfeller lagt til grunn at innsamling, lagring og systematisering av opplysninger om enkeltpersoner fra offentlige myndigheter er omfattet av EMK artikkel 8.[2] I EMDs dom *Segerstedt-Wiberg and Others v. Sverige*[3] ble det også lagt til grunn at systematisk innsamling og lagring av offentlig tilgjengelig informasjon av myndighetene utgjorde et inngrep i EMK artikkel 8. Når det gjelder informasjon om enkeltpersoner i den offentlige sfære, har EMD fastslått at det er en «*zone of interaction between a person with others, even in a public context, which may fall within the scope of "private life*».[4] I denne konteksten vil hvilke

[2] Rotaru v. Romania (28341/95) avsnitt 44

[3] Segerstedt-Wiberg and Others v. Sverige (62992/00) avsnitt 72 og 73.

[4] EMDs dom Gillan and Quinton v. Storbritannia (4158/05) avsnitt 61 og P.G og J.H v. Storbritannia (44787/98) avsnitt 56. Se også Rotaru v. Romania avsnitt 43, «Moreover, public information can fall within the scope of private life where it is systematically collected and stored in files held by the authorities. That is all the truer where such information concerns a person's distant past".

forventninger en person har til privatliv være en sentral faktor, selv om dette ikke er avgjørende.[5]

EMD har ikke behandlet spørsmålet om bulkinnsamling av åpne kilder. Domstolen har imidlertid i storkammerdommene *Big Brother Watch v. Storbritannia* og *Centrum för Rättvisa v. Sverige* tatt stilling til de menneskerettslige kravene som må stilles til bulkinnsamling av signal-etterretning.[6] Etter NIMs syn gir EMD-dommene i noen grad veiledning på hvilke krav som stilles til den type innsamling og behandling som forslaget legger opp til.

Inngrep i retten til privatliv vil etter EMK artikkel 8 nr. 2 kun være tillatt dersom tre vilkår er oppfylt. Sammenfattet kreves det at (i) inngrepet må ha hjemmel i lov, (ii) inngrepet må søke å ivareta et legitimt formål og (iii) inngrepet må være nødvendig (herunder forholdsmessig) for å ivareta formålet.

Formålet om å avdekke ukjente trusselaktører, kartlegge utviklingen i trusselbildet og oppdage nye fenomener som kan medføre nye trusler, er legitime formål i konvensjonens forstand.[7]

I saker om overvåking vurderer EMD gjennomgående forholdsmessighetskravet og lovkravet under ett.[8] Dette innebærer blant annet at regelverket må inneholde rettssikkerhetsmekanismer som sikrer at overvåkingskapasiteten kun brukes dersom det er nødvendig. Nødvendighetsvilkåret ligger ifølge praksis fra EMD et sted mellom «uunnværlig» på den ene siden og «ønskelig» eller «nyttig» på den andre. Vurderingen må foretas konkret og helhetlig, der viktige rettesnorer er om inngrepet er egnet til å nå formålet, om formålet kan nås med mer lempelige midler (minste inngreps prinsipp), og om inngrepet svarer til et «tvingende samfunnsmessig behov».[9] Endelig vil dette bero på hvorvidt inngrepet totalt sett er forholdsmessig sett hen til formålet. Forholdsmessighetsavveiningen munner ofte ut i et spørsmål om myndighetene har funnet en «rimelig balanse» mellom formålet (behovet for inngrepet) på den ene siden og individets rettigheter på den andre.[10]

I vurderingen av om myndighetene har funnet en rimelig balanse, er det i slike saker sentralt om systemet og regelverket inneholder gode kontrollmekanismer og rettssikkerhetsgarantier for å minske risikoen for blant annet misbruk, vilkårlighet og formålsutglidning. Basert på inngrepets karakter og styrke, kan

[5] Benedik v. Slovenia (62357/14) avsnitt 101.

[6] Se blant annet Big Brother Watch and Others v. Storbritannia (58170/13 62322/14 og 24960/15) og Centrum för rättvisa v. Sverige (35252/08).

[7] Se f. eks. Big Brother Watch and Others v. Storbritannia avsnitt 365.

[8] Se f. eks Roman Zahkarov v. Russland (47143/06) avsnitt 232.

[9] Se f. eks Breyer v. Tyskland (50001/12) avsnitt 88

[10] Ibid. avsnitt 91.

rettssikkerhetsgarantiene blant annet knytte seg til bruken av materialet, lagringstiden, sletting og mulighetene for klage/overprøving. I saker hvor myndighetene tillates å innhente opplysninger som angår borgernes privatliv uten at borgerne får kjennskap til innsamlingen, har EMD i sin praksis innfortolket et krav til effektiv og uavhengig kontroll for å hindre myndighetsmisbruk. Hvilke krav som skal stilles til kontroll, vil til en viss grad bero på hvor inngripende et slikt tiltak anses for å være.

Etter EMDs praksis har myndighetene relativt vid skjønnsmargin til å vurdere hvilke tiltak og overvåkingssystemer som anses nødvendige for å beskytte nasjonale interesser. Det er likevel sentralt at tiltakene har tilstrekkelige rettssikkerhetsmekanismer. NIM mener at høringsnotatet ikke i tilstrekkelig grad berører hvor tyngende inngrepet er, og hvilke rettssikkerhetsmekanismer som bør ledsage forslaget for at tiltaket skal kunne anses som forholdsmessig. Etter NIMs oppfatning bør rettssikkerhetsmekanismene forbedres vesentlig før tiltaket eventuelt kan iverksettes.

I det følgende vil NIM vurdere forslaget opp mot kriteriene som kan utledes fra EMDs praksis om lignende tiltak hvor informasjon fra borgerne samles inn og brukes av hensyn til bekjempelse av kriminalitet og terror.

3.2. Inngrepets art og begrunnelse

Et utgangspunkt for vurderingen av om myndighetene har funnet en rimelig balanse mellom formålet på den ene siden og individets rettigheter på den andre, er hvor inngripende tiltaket er. Departementet skriver at det foreslåtte tiltaket er en grunnleggende forutsetning for at PST skal kunne ivareta oppgaven med å kartlegge trender og utviklingstrekk og utarbeide analyser og etterretningsvurderinger av betydning for bekjempelsen av alvorlig kriminalitet.[11] Departementet skriver at forslaget skiller seg fra tilrettelagt innhenting, bruk av skjulte tvangsmidler og andre inngripende overvåkingsmetoder.[12] Departementet vurderer at vid innsamling av åpne kilder er mindre alvorlig enn bruk av denne typen metoder. Departementet konkluderer derfor med at PSTs samfunnsoppdrag samt reglene om informasjonssikkerhet, internkontroll og sporing oppveier risikoen for en eventuell nedkjølende effekt,[13] og videre at rettspraksis om de særskilte rettssikkerhetsmekanismene ved skjulte bulkovervåkingsmetoder kun i begrenset grad gjør seg gjeldende.

Etter NIMs oppfatning underkommuniserer høringsnotatet hvor inngripende tiltaket er. Forslaget i høringsnotatet er omfattende, særlig sett i lys av at det både utvider PSTs oppdrag til mer generell etterretningsvirksomhet og samtidig utvider adgangen til innsamling, analyse og uthenting og bruk av åpen informasjon. Dette innebærer at nær

[11] Høringsnotatet s. 21.

[12] Høringsnotatet s. 21.

[13] Høringsnotatet s. 25.

sagt alt som publiseres åpent på internett vil kunne samles inn og lagres hos PST i 15 år. Lagringsadgangen gjelder også der materialet i mellomtiden er fjernet fra internett. Videre gjelder muligheten til innsamling uavhengig av om den enkelte er mistenkt for et straffbart forhold eller ikke.

Departementet foreslår ingen begrensninger i hva som kan samles inn, så lenge opplysningene er «åpent tilgjengelig». Opplysningene kan videre systematiseres og sammenstilles på en måte som er uoversiktlig for den enkelte. Informasjonen kan også omfatte informasjon som senere er blitt slettet.

Departementet skriver på side 22 i forslaget at data fra sosiale medier vil være offentlig tilgjengelig data som brukere frivillig har lagt ut. Det er imidlertid ikke gitt at informasjon som er gjort offentlig tilgjengelig, er frivillig lagt ut. Svært mye av det som publiseres på sosiale medier vil omfatte opplysninger som er lagt ut av tredjepersoner, og hvor den omtalte ikke kjenner til publiseringen. Det kan også tenkes tilfeller hvor informasjon er delt mot noens vilje, eksempelvis fordi kontoer er hacket eller passord er kommet på avveie. Det må videre legges til grunn at den enkelte ikke har oversikt over opplysninger som har blitt lagt ut på sosiale medier bakover i tid. Når det ikke settes begrensninger, innebærer det at enhver i realiteten må gå ut ifra at alt vedkommende skriver, vil kunne lagres hos PST. Dette omfatter etter forslaget også sensitive personopplysninger, slik som politiske oppfatninger samt mer personlig informasjon som fremkommer eksempelvis på sosiale medier. Det er dessuten ikke foreslått avgrensninger mot opplysninger som omhandler barn. Både de som publiserer og de som omtales kan være mindreårige. Forslaget vil derfor kunne utgjøre et inngrep i barns rett til privatliv og ytringsfrihet. Merverdien ved at PST skal samle alt som er publisert fremstår ikke tilstrekkelig begrunnet i høringsnotatet.

NIM er enig med departementet i at det i mange tilfeller ikke er tale om innsamling av informasjon hvor den som publiserer har en forventning om at det som publiseres også skal være skjult. Det er nærmest åpenbart at den som publiserer ikke har en slik forventning i normaltilfellene. En slik forventning kan likevel ikke være avgjørende for hvor inngripende tiltaket anses å være. At informasjon er åpent tilgjengelig er ikke ensbetydende med at den omhandlede ikke har noen beskyttelsesverdig interesse i, eller forventning om, at *alt* som publiseres ikke samles og sammenstilles av offentlige myndigheter. En så omfattende innsamling kan også ha en nedkjølende effekt, jf. drøftelsen av ytringsfrihet nedenfor under punkt 5. Å unngå en nedkjølende effekt er et samfunnsmessig tema som ikke avklares tilstrekkelig ved å spørre om forventningene ved den enkelte konkrete publisering. Man kan derfor ikke generelt slutte at en så omfattende innsamling av åpne kilder alltid har mindre konsekvenser for privatlivet. NIM mener derfor at departementets «fra det mer til det mindre»-betraktninger fra inngripende individuelle overvåkingstiltak til bred innsamling av åpne kilder, ikke utgjør

noen hensiktsmessig tilnærming for å fastslå inngrepsgraden. Spørsmålet må være hvor inngripende dette tiltaket faktisk er.

I NOU 2009:15 uttalte Metodekontrollutvalget følgende om forskjellen mellom individuell og generell overvåkning:

> «[d]*en generelle formen for overvåking reiser etter utvalgets oppfatning enda større og mer fundamentale spørsmål i relasjon til de verdier som ligger til grunn for personvernet – individets behov for en privat sfære der det kan utvikles både som menneske og som deltaker i de demokratiske prosesser – enn politiets bruk av skjulte tvangsmidler*».[14]

Departementet viser heller ikke til forskjellen mellom innsamling av informasjon fra utenlandske aktører og innsamling av informasjon fra egne borgere. Begrensninger på masseinnsamling av opplysninger om egne borgere vil som et klart utgangspunkt redusere handlingsrommet til sikkerhetsmyndighetene sammenlignet med innsamling rettet mot utenlandske forhold, og samtidig stille skjerpede krav til sikkerhetsmekanismer.[15] PST uttalte til illustrasjon i sitt høringssvar til den nye etterretningstjenesteloven at «[...] den delen av Etterretningstjenestens metodebruk som berører personer eller virksomheter innenfor norsk jurisdiksjon, bør underlegges domstolskontroll».[16]

Samlet sett anser NIM forslaget langt mer inngripende enn høringsnotatet reflekterer. Masseinnsamling av data fra internett vil utfordre grunnleggende menneskerettigheter, som retten til privatliv, personvern og ytringsfriheten. I tillegg til selve innsamlingen, vil de ulike stadiene i behandlingen etter innsamlingen, herunder manglende forhåndskontroll ved søk, og den vide adgangen for bruk og analyse av opplysningene, forhøye inngrepets grad ytterligere. Adgangen til utstrakt bruk av automatiserte analyseverktøy og en lagringstid på hele 15 år forsterker inngrepsgraden ytterligere.

Balanseringen mellom sentrale menneskerettigheter og demokratiske verdier på den ene siden og samtidig ønske om å utstyre myndighetene med nødvendige verktøy for å sikre PSTs samfunnsoppdrag på den andre siden, er en vanskelig avveining. Det er klart at bulkinnsamlingssystemer innebærer en reell risiko for at grunnleggende rettigheter krenkes. EMD formulerer dilemmaet slik: «*a system of secret surveillance for the protection of national security may undermine or even destroy democracy under the cloak of defending it*».[17]

---

[14] NOU 2009:15 s. 129.

[15] Se Big Brother Watch and Others v. Storbritannia, avsnitt 374 – 376.

[16] Høringssvar fra PST – Forslag til ny lov om Etterretningstjenesten, 12. februar 2019, s. 4.

[17] Se blant annet Centrum för Rättvisa v. Sweden avsnitt 253, Big Brother Watch and Others v. Storbritannia avsnitt 339 og Weber and Saravia v. Tyskland (54934/00) avsnitt 106.

3.3. Overføringsverdien av EMDs dommer om bulkinnsamling

I to nylig avsagte storkammerdommer om bulkovervåkingssystemer, konkluderte EMD med at bulkinnsamling ikke i seg selv utgjorde et uforholdsmessig inngrep i retten til privatliv, under forutsetning av at omfattende rettsikkerhetsmekanismer i alle stadier av prosessen, var til stede. I begge sakene var det tale om bulkinnsamling av blant annet kommunikasjonsdata som ikke var rettet mot enkeltpersoner. EMD la til grunn at statene hadde vid skjønnsmargin i valget av hvilke systemer som skal iverksettes for å sikre nasjonal sikkerhet, men at det var sentralt hvorvidt systemet inneholdt effektive garantier mot misbruk i vurderingen av om inngrepet var i tråd med EMK artikkel 8.[18]

EMD er relativt intensiv i prøvingen av om et system som overvåker innbyggere er innrettet med rettssikkerhetsgarantier som sikrer at systemet ikke misbrukes. Dette er en sentral del av forholdsmessighetsvurderingen for overvåkingssystemer.

Departementet fremhever at EMDs praksis ikke omhandler åpne kilder, og konkluderer med at EMDs avgjørelser derfor har liten overføringsverdi. NIM har et annet syn. Det forhold at forslaget gjelder åpne kilder kan også medføre at det stilles andre eller strengere krav. Ved åpne kilder er det ikke tilstrekkelig å ta utgangspunkt i hvilken forventning som forelå ved publiseringen. Som nevnt ovenfor må man vektlegge videre samfunnsmessige hensyn. Videre omhandler EMD-dommene behandling av data helt fra innsamling til sletting.

NIM mener at den tilsynelatende vide innsamlingsadgangen, lange lagringstiden, vide rammer for bruk, kombinert med bruken av automatiserte analyseverktøy tilsier at forslaget må møtes med strengere regler for lagring og andre rettssikkerhetsgarantier for å kunne anses forholdsmessig.

Som departementet er inne på, er det vesentlige ulikheter mellom bulkovervåkingssystemene EMD har tatt stilling til, og dette forslaget. De to EMD-avgjørelsene handler om bulkovervåking av kommunikasjonstrafikk, metadata og innholdsdata, som krever skjult tilgang til signaloverføringsenheter. Dette forslaget dreier seg derimot om innsamling av informasjon fra åpent tilgjengelige kilder. Det er som nevnt i høringsbrevet og drøftet ovenfor, tale om opplysninger som den enkelte i mange tilfeller vil ha mindre forventning om å holde skjult, enn opplysninger fremkommet ved kommunikasjonskontroll.

Etter NIMs oppfatning er det særlig *innsamlingsmåten* og hvilke opplysninger som skal samles inn, som skiller forslaget fra sakene om tilrettelagt innhenting. Selv om selve innsamlingsmetoden er ulik, vil forvaltning, sammenstilling, analyse, lagring samt senere bruk av dataene i mindre grad skille seg fra problemstillingene i EMD-dommene, hvor poenget er å forhindre misbruksfaren som alltid foreligger ved slike personverninngrep.

[18] Se Big Brother Watch and Others v. Storbritannia, avsnitt 360.

Det gjør seg gjeldende også her. Etter forslaget kan opplysningene analyseres ved hjelp av automatiserte analyseverktøy, uten at dette spesifiseres ytterligere. Bruk av analyseverktøy kan frembringe nye mønstre og ny informasjon med utgangspunkt i de åpne kildene. Denne informasjonen kan være gjenstand for feilslutninger, og den kan ikke imøtegås. Problemstillingene som oppstår etter at opplysningene er samlet inn skiller seg følgelig i mindre grad fra problemstillingene i EMD-dommene.

Et annet og sentralt element, er at dette forslaget åpner for et system som er egnet til å overvåke *egne* borgere, og ikke personer som befinner seg i utlandet. At staten utfører etterretning rettet personer i Norge er generelt sett langt mer inngripende enn der de utfører etterretning overfor aktører i utlandet, fordi staten har langt større maktmidler som kan benyttes overfor egne borgere. Videre er misbrukspotensialet langt større ved innsamling rettet mot egne borgere enn utenlandske borgere. Vi kan ikke se at disse sentrale momentene er berørt i høringsnotatet.

NIM mener at departementets analyse av EMDs rettspraksis om masseovervåking og bulkinnsamling er mangelfull. Selv om det er visse forskjeller mellom de to systemene, er det også mange likheter, slik påpekt foran. Forskjellene kan dessuten tilsi en annen eller bredere drøftelse. Det kan ikke utledes direkte av EMDs praksis at prinsippene for bulkovervåking *ikke* kan komme til anvendelse for innhenting fra åpne kilder. Etter NIMs oppfatning må en slik avgrensning hvile på en mer inngående analyse av rettspraksis holdt opp mot dette forslaget, særlig hva gjelder inngrepets art samt begrunnelsen og behovet for rettssikkerhetsgarantier under hvert enkelt stadium av behandlingen. NIM etterlyser også i hvilken grad departementet mener rettspraksisen kan få overføringsverdi for forslaget, og en begrunnelse for dette. Etter NIMs syn er det også mange likhetstrekk som indikerer at det bør iverksettes ytterligere rettsikkerhetsmekanismer enn forslaget legger opp til. Hvilke kontrollmekanismer som iverksettes har betydning for forholdsmessigheten av tiltaket.

I *Big Brother Watch* stilles det opp åtte kriterier for bulkovervåkningssystemer.[19] Dette gjelder i korte trekk på hvilket grunnlag og for hvilke formål innhentingen kan autoriseres, hvilke omstendigheter som kan medføre innhenting av enkeltpersoners kommunikasjon, prosedyrer for autorisasjon, prosedyrer for utvelgelse, analyse og bruk av data, forholdsregler ved utlevering til andre, tidsbegrensninger, lagring og sletting av innhentede data, prosedyrer for uavhengig etterhåndskontroll, og kontrollorganets kompetanse.

Videre legger dommen opp til en samlet vurdering. Etter NIMs syn har flere av prinsippene oppstilt i dommen overføringsverdi til dette tilfellet. Vi kommer nærmere tilbake til sikkerhetsmekanismene i forslagets enkelte deler nedenfor.

[19] Avsnitt 361.

4. Lovforslagets enkelte deler

4.1. Innledning

Vi har ovenfor gjort rede for våre generelle syn på rammene for forslaget, inngrepets art og i hvilken grad vi mener EMDs dommer knyttet til bulkinnsamling har overføringsverdi til dette forslaget. Som det fremkommer, mener vi at forslaget må innrammes av betydelige sterkere rettsikkerhetsmekanismer, og at det må gjøres grundigere drøftelser av forholdet til menneskerettighetene, for at det skal kunne vedtas. I det følgende gis en nærmere redegjørelse for NIMs syn på forslagets ulike punkter.

4.2. Lovfesting av PSTs etterretningsmandat

Forslaget søker å klargjøre PSTs rolle som innlands etterretningstjeneste, og departementet ber om høringsinstansenes syn på dette.

PSTs oppdrag etter politiloven er beskrevet som forebygging og etterforsking av konkrete angitte straffbare handlinger. Tjenesten har derfor begrenset mulighet til å behandle informasjon for å bidra med generelle etterretningsoppgaver og analyser knyttet til trender og utvikling i trusselbildet i Norge. Forslaget legger opp til at PST får en klar hjemmel til etterretningsoppdrag i Norge, og at informasjon for dette formålet kan samles inn med hjemmel i politiregisterloven. NIM støtter at PSTs rolle og oppgaver klargjøres, men etterlyser en grundigere gjennomgang av de menneskerettslige effektene en slik utvidelse av PSTs overvåkning i Norge kan føre med seg, særlig knyttet til retten til privatliv, personvern og retten til ytringsfrihet.

4.3. Behandling av åpent tilgjengelig informasjon

4.3.1. Virkeområdet – hva som kan samles inn

Departementet foreslår ingen begrensninger i hva som kan samles inn, så lenge opplysningene er «åpent tilgjengelig». Begrepet er ikke nærmere definert eller avgrenset utover at det ikke skal kreve «forsering av passord eller lignende beskyttelsesmekanismer». Hva som skal anses som åpent tilgjengelig er slik NIM forstår derfor all informasjon, om hvem som helst, uten hensyn til medium eller publiseringsmåte. Adgangen skal etter høringsnotatet også omfatte informasjon på det mørke nettet.

Forslaget åpner altså for innsamling av personopplysninger og annen informasjon om enhver, uten at de noen gang har vært eller vil være i politiets søkelys. Dette kan derfor inkludere sensitive personopplysninger slik som helseopplysninger, opplysninger om politisk oppfatning, og opplysninger om en persons legning. Videre vil det også kunne inkludere offentlig tilgjengelige opplysninger som kan være feilaktige eller misvisende, opplysninger som er tilveiebrakt eller publisert ulovlig, og opplysninger publisert om enkeltpersoner uten deres kjennskap eller samtykke. Dette er opplysninger som vil

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

Forslaget åpner for å lagre all informasjon, uten nødvendighetsbegrensning. Det vil også omfatte store mengder informasjon som er helt uten betydning for PST.

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

> «*Våre holdninger til hva som er å regne som privat og offentlig forandres kontinuerlig. Særlig kan det på sosiale medier være vanskelig å skille privat fra offentlig. Hvordan bestemmer vi hva som er "offentlige rom", hva som er "private rom" og hva som muligens er en ny hybrid mellom offentlig og privat. Det finnes mange ulike sosiale medier, og de opererer på ulike måter. Noen er helt åpne, noen krever registrering og pålogging for å kunne se innhold, mens andre opererer med ulike fora hvor noen er mer åpne og andre mer lukkede. Facebook er stort nettsamfunn som krever pålogging. Deler av informasjonsutvekslingen er åpen for alle, mens andre deler skjer i mer lukkede fora. Hvorvidt informasjon i sosiale medier deles bredt eller ikke, bestemmes dels av tjenesten, og dels gjennom bevisste valg brukeren gjør gjennom innstillinger tilbudt av tjenesten. Etter hvert som slike innstillinger blir mer komplekse og standardinnstillinger rigges mot aktiv og bred deling, er det imidlertid urimelig å anta at alle brukere til enhver tid er bevisst på hvor mye og hvor bredt informasjonen faktisk deles"*[20]

Det er heller ikke omtalt i høringsnotatet om PST etter forslaget vil kunne benytte seg av falske identiteter eller brukere på nett for å få tilgang til informasjon som en bruker av sosiale medier kun deler med venner, følgere eller liknende avgrenset krets. Dette er en type sperring som bør omtales og reguleres tydelig, idet det etter forslaget ikke er åpenbart om aktiv fordekt opptreden omfattes av formuleringen «*passord eller liknende*

[20] Teknologirådets rapport På nett med publikum (2014), s. 67

beskyttelsesmekanismer». Aktivt fordekt opptreden er eksplisitt inntatt som begrensning i etterretningstjenesteloven § 6-2.

Når det gjelder avgrensning mot lagring av sensitive personopplysninger, har dette ikke annen begrunnelse enn at det ikke vil være mulig å skille ut disse opplysningene. NIM savner en mer grundig redegjørelse for betenkelighetene med en slik innsamling, både av hensyn til personvernet og av hensyn til ytringsfriheten. For den enkelte kan det oppleves svært belastende om PST samler inn denne typen opplysninger. Videre savner NIM en omtale av om det kan innføres mekanismer for å unngå betenkelighetene ved å innsamle slike opplysninger. Det er eksempelvis ikke innført eller diskutert noen begrensninger knyttet til *bruk* av disse opplysningene, selv om dette må antas å være mer teknisk mulig enn å skille disse ut allerede i innsamlingsfasen, jf. også nedenfor.

Etter NIMs oppfatning bør det vurderes om adgangen til innsamling av opplysninger bør presiseres og konkretiseres nærmere. Dette også i lys av manglende forhåndskontroll med hva som kan hentes ut, muligheten for generering av ny informasjon ved hjelp av automatiske analysesystemer, og det vide formålet opplysningene kan brukes til, jf. nedenfor under pkt. 4.3.2.

4.3.2. Virkeområdet – hva opplysningene kan brukes til

I EMDs praksis om bulkinnsamling er det i forholdsmessighetsvurderingen relevant hvilke prosedyrer som er på plass for utvelgelse, undersøkelse og bruk av innsamlet materiale.[21]

Forslaget i ny § 65 a annet ledd angir at opplysningene kan brukes til følgende tre formål:

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

Alternativet i nr. 1 om etterretningsvirksomhet har et vidt angitt virkeområde. Som departementet selv er inne på i høringsnotatet, er «etterretning» ikke en entydig rettslig størrelse. Alternativet krever ingen forutgående kontroll eller godkjenning utover at personen som foretar søket skal ha særskilt bemyndigelse. Hvem eller hvordan det skal avgjøres om bruken kan rubriseres som «etterretningsvirksomhet», er ikke angitt.

NIM forstår departementet dithen at alternativet «etterretning» blant annet skal omfatte innhenting, analyse og vurdering av informasjon, eksempelvis med formål å forebygge straffbare forhold, men også forut for det som tradisjonelt omfattes av

[21] Big Brother Watch v. Storbritannia avsnitt 384-391.

begrepet forebygging. Det er vanskelig for befolkningen å skulle overskue konsekvensene av dette, all den tid det er vanskelig å avgjøre hva som omfattes av begrepet «etterretning».

Alternativ 2 om opprettelse av eller bruk i forebyggende sak er også vidt, og vil også åpne for utstrakt søk i materialet også dersom man ønsker å undersøke om forebyggende sak overhodet skal opprettes. NIM forutsetter at vilkårene i politiregisterloven § 64 første ledd bokstav a) uansett må være oppfylt, og at søkene som utføres må stå i saklig sammenheng med det som danner grunnlaget for å utføre undersøkelsen i § 64 første ledd bokstav a). At søket må ha en slik saklig sammenheng kan med fordel presiseres i lovteksten.

Etter alternativet i nr. 3 kan opplysningene også brukes i etterforsking av lovbrudd under PSTs ansvarsområde. Dette innebærer, i motsetning til eksempelvis etter e-tjenesteloven, at opplysningene både kan brukes til etterretning og forebyggingsformål, i tillegg til som ledd i etterforskningen og eventuell senere bevisførsel i straffesaker.

Samlet betyr de tre alternativene at opplysningene som er samlet i realiteten kan benyttes til samtlige av PSTs ansvarsområder. Dette gir en svært vid adgang til bruk av opplysningene, uten reell avgrensning, og uten forutgående kontroll. Etter NIMs oppfatning gir en såpass vid adgang til bruk av opplysningene grunn til å anse inngrepet som langt mer omfattende enn dersom formålet kun var å kartlegge trender og «følge med på internett».[22]

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

Departementet burde videre understreket tydeligere hvordan PST skal unngå at søk i materialet blir tilfeldig, gitt at formålet er såpass vidt. Dette har også en klar side til å unngå misbruk og formålsutglidning. En tydeligere avgrensning vil også gi borgerne mulighet til å forutse når opplysningene kan hentes ut. Endelig er en tydeligere avgrensning en forutsetning for at kontrollorganer skal kunne føre noen meningsfull kontroll med hva som er lovlig lagring og bruk- og hva som ikke er det, jf. nedenfor under punkt 4.3.6.

4.3.3. Automatiserte analyseverktøy

Departementet åpner for at behandling for etterretningsformål kan skje ved bruk av automatiserte analyseverktøy. Det er ikke nærmere spesifisert hva slags analyseverktøy som kan benyttes, eller hvordan disse skal innrettes. NIM legger til grunn at

[22] Høringsnotatet s. 2.

automatiserte analyseverktøy vil kunne omfatte verktøy basert på maskinlæring/kunstig intelligens, selv om dette ikke er uttrykkelig nevnt i høringsnotatet.

En iboende risiko ved automatiserte analyseverktøy er diskriminering og forutinntatthet.[23] I EU-kommisjonens etiske retningslinjer for kunstig intelligens, som også ligger til grunn for Nasjonal strategi for kunstig intelligens, anbefales blant annet at kunstig intelligens som bygger på personopplysninger, eller som retter seg mot personer, skal følge personvernforordningen. Videre anbefales det at identifiserbare og diskriminerende skjevhet bør fjernes i innsamlingsfasen av datasett.[24]

Bruk av slike verktøy for kriminalitetsbekjempelsesspørsmål reiser særlige spørsmål. I Nasjonal strategi for kunstig intelligens skisseres utfordringsbildet slik:

> *«Et område som reiser flere dilemmaer er bruk av KI til kontrollformål. Slik kontroll kan for eksempel være å identifisere personer som kan tenkes å bryte regelverket (det vil si der algoritmen identifiserer en høy sannsynlighet for dette). For slike anvendelser må det vurderes om rettsikkerheten og vernet mot selvinkriminering for den som kontrolleres ivaretas. Risikoen for, og konsekvensene av, falske positive – altså at noen blir feilaktig utpekt og den belastningen dette medfører for den det gjelder – må være en del av personvernvurderingen, som må inngå når en løsning utredes.»*

Teknologirådet har videre uttalt følgende:

> *«Hvis automatiserte dataanalyser blir viktigere som beslutningsstøtte i justissektoren, blir det samtidig viktig å kontrollere og forstå hvordan beslutningene kommer til veie. Justisdepartementet bør sørge for at det utføres jevnlige tilsynskontroller av algoritmene og analysene som politiet bruker i sitt arbeid. Det er viktig for at man skal kunne forsikre seg om at politiet bruker analysene riktig, opererer innenfor lovverket og ivaretar personvernet i alle ledd. En slik åpenhet er ikke minst viktig for at politiet skal opprettholde sin tillit i befolkningen. Et eksternt, uavhengig og teknisk kyndig tilsyn bør få tilgang til politiets data- og analysesystemer for å vurdere hvorvidt politiet bruker robuste og kvalitetssikrede data, systemene opererer innenfor lovverk og gjeldende retningslinjer, [og om] algoritmene inneholder skjevheter, usikkerheter, subjektive vurderinger eller tilfeldige valg som kan bidra til å systematisere utilsiktede konsekvenser som f.eks. diskriminering.»*[25]

Ved at nær sagt alt som er publisert gjennom åpne kilder vil kunne samles inn av PST, må det legges til grunn at også ulovlig, uriktig eller villedende informasjon vil kunne

---

[23] Dette er eksempelvis lagt til grunn i Nasjonal strategi for kunstig intelligens.

[24] Se Nasjonal strategi s. 58-60.

[25] Teknologirådets rapport Forutseende politi (2015) s. 11.

samles inn. Dette kan igjen påvirke analysene som gjøres, både av automatiserte verktøy og ved manuell behandling. EMD har generelt uttalt at «*the need for safeguards will be all the greater where the protection of personal data undergoing automatic processing is concerned*".[26]

Etter NIMs oppfatning bør automatiske analyseverktøy bygge på etiske prinsipper, og utformes med tanke på menneskerettighetene. NIM savner i lys av disse grunnleggende utfordringene en nærmere beskrivelse av analyseverktøyene, hvordan disse tenkes brukt, herunder hvilke mekanismer som er tenkt iverksatt for å forhindre og redusere diskriminering, misvisende resultater eller andre uønskede utfall ved bruk av slike verktøy, herunder falsk og villedende informasjon.

Dersom PSTs beslutning i en gitt sak er basert på vurderingen fra et automatisert analyseverktøy, bør dette i alle tilfeller fremgå tydelig av beslutningen.

4.3.4. Sperring

Etter forslaget til ny § 65 a annet ledd skal opplysningene sperres. Sperring vil etter NIMs syn bidra til å sikre at opplysningene holdes atskilt og ikke benyttes i større utstrekning enn loven gir anvisning på. Samtidig gir loven etter NIMs oppfatning en svært vid adgang til å innsamle og benytte opplysningene, jf. foran, og lite begrensninger på hvilke personer som kan få tilgang til dem, jf. nedenfor. Dette reduserer vekten av sperring som et egnet sikkerhetstiltak.

4.3.5. Saksbehandling og kontroll – bemyndigelse

Etter forslaget i politiregisterforskriften § 21-8 første ledd skal tilgang til innsamlede opplysninger kun gis til personer med særskilt bemyndigelse. Det fremgår ikke hva som skal til for å få slik bemyndigelse. Det foreslås heller ikke et krav om at tilgangen skal begrenses til så få personer som mulig, selv om det forutsettes i høringsnotatet at tilgang ikke gis til flere personer enn nødvendig. Denne forutsetningen fremgår ikke av bestemmelsen, og vil derfor ikke ha tydelig rettslig forankring. NIM mener en slik forutsetning bør reguleres positivt.

4.3.6. Særlig om uavhengig kontroll og søkekriterier

EMD er intensiv i prøvingen av om et overvåkingssystem inneholder tilstrekkelige kontrollmekanismer. Kontrollen bør etter EMD ligge til den dømmende virksomhet i saker om skjult overvåking.[27] Tilsvarende doktriner er utviklet for saker om bulkinnsamling av data.[28] For at slike systemer skal være forholdsmessig må forslaget

[26] Se Big Brother Watch and Others v. Storbritannia avsnitt 330, med videre henvisninger.

[27] Klass mfl. v. Tyskland (5029/71) avs. 55-56 og Kennedy v. Storbritannia (26839/05) avs. 167. Roman Zahkarov v. Russland avsnitt 233.

[28] Big Brother Watch and Others v. Storbritannia.

ledsages av rettssikkerhetsgarantier som motvirker misbruksrisikoen ved bulkinnsamlingssystemer og ivareta kravet til forutberegnelighet.

Slik vi har redegjort for ovenfor, anser NIM at forslaget om masseinnsamling og behandling av opplysninger fra åpne kilder utgjør et større inngrep enn hva departementet legger til grunn. Høringsnotatet kunne med fordel beskrevet nærmere hvordan opplysningene skal behandles, utover at opplysningene skal slettes etter 15 år.

NIM bemerker at forslaget ikke inneholder noen begrensninger på hvordan søk skal foregå eller gjennomføres. Høringsnotatet burde inneholdt avgrensninger av hvilke søkekriterier som kan benyttes, og mekanismer for å sikre at disse står i saklig sammenheng med formålet opplysningene skal uthentes for. Hvilke søkebegrep som brukes kan være avgjørende for om en konkret bruk av informasjonen er forholdsmessig eller ikke. Det er generelt et sentralt poeng at rettssikkerhetsmekanismene må fungere i praksis, herunder at garantiene mot misbruk bygges inn i systemet, og at det foreligger reelle avgrensninger av hvilke søkekriterier som kan benyttes. Slik forslaget er lagt opp, mener NIM at det gir PST en ubestemt skjønnsmyndighet uten kriterier for overprøving. Dette gjør også den foreslåtte kontrollen av søk lite effektiv som kontrollmekanisme, ettersom skillet mellom lovlig og ikke lovlige søk, ikke er tydelig.

Samlet mener NIM at departementets begrunnelse for å ikke innføre forhåndskontroll når det skal gjennomføres søk i det innsamlede materialet, ikke er tilfredsstillende. På bakgrunn av den vide innsamlingsadgangen og den lange lagringstiden anbefaler NIM at departementet i tillegg legger til rette for forhåndskontroll når det foretas søk i det innsamlede materialet. Dette kan eventuelt gjøres ved at det innføres en godkjenningsordning for hvilke opplysninger, søkeord eller andre parametere som kan ligge til grunn for søk i materialet.

4.3.7. Slettefrist

Etter lovforslaget skal opplysningene slettes senest etter 15 år. Departementet har bedt om høringsinstansenes syn på slettefristen.

I EMDs praksis om bulkinnsamling er begrensninger i lagring av innsamlet materiale, og under hvilke omstendigheter slikt materiale må slettes, et relevant moment i vurderingen av et tiltaks forholdsmessighet.[29] Også i saker om annen lagring av personopplysninger har det vært vurdert hvorvidt lagringstiden går lenger enn hva som er nødvendig.[30]

Etter NIMs oppfatning vil inngrepet være større jo lengre lagringstid det åpnes for, samtidig som det reelle behovet for opplysningene gjerne vil være redusert. De færreste

[29] Se Big Brother Watch and Others v. Storbritannia avsnitt 400-405.

[30] Se f.eks. S. and Marper v. Storbritannia (30562/04 og 30566/04), B.B. v. Frankrike (5335/06), Gardel v. Frankrike (16428/05), M.B. v. Frankrike (22115/06) og M.K. v. Frankrike (19522/09).

har oversikt over hva som ble publisert om dem for mange år tilbake. Risikoen for formålsutglidning i hva opplysningene kan brukes til vil også øke jo lenger lagringstid det er tale om. Befolkningen må da ikke bare ha tillit til at PST i dag kun benytter opplysningene til det de er innhentet for, men også at senere styresmakter ikke vil utvide rammene for når og hvordan disse kan anvendes. En lang lagringstid vil kunne øke denne bekymringen. Også øvrige rettssikkerhetshensyn, slik som muligheten for å verifisere opplysningenes sannhet, kan gjøre lang lagringstid mer betenkelig. Retten til kontradiksjon vil også kunne vanskeliggjøres dersom den enkelte ikke husker når eller i hvilken kontekst noe ble publisert. Det er heller ikke gitt noen nærmere redegjørelse for behovet for en såpass lang frist som 15 år.

Departementet skriver i høringsnotatet at fristen er en «lengstefrist». Så lenge forslaget ikke inneholder noen plikt til å revidere og slette materialet innenfor denne fristen må det imidlertid legges til grunn at store deler av innsamlede opplysninger vil beholdes ut lengstefristen.

NIM mener på denne bakgrunn at den foreslåtte fristen på 15 år er altfor lang.

4.3.8. Politiregisterforskriften – registrering og sporing

I forslaget til ny § 21-8 i politiregisterforskriften er det foreslått at bruken av opplysningene skal kunne registreres og spores for å kunne kontrollere om søkene og bruken er tillatt eller ikke. Det angis i bestemmelsen at dette skal skje «*regelmessig*».

Et sentralt prinsipp for masseinnsamling av opplysninger, er at regelverket og systemet ivaretar kravet til åpenhet og forutberegnelighet. Etter NIMs oppfatning er misbruks- og skadepotensialet ved uautorisert bruk av materialet stort, og slik uautorisert tilgang kan ramme enkeltmennesker særlig hardt. Ettersom forslaget inneholder få begrensninger i hvilke opplysninger som kan samles inn, og hvordan de kan behandles og hentes ut, vil kontrollen etter § 21-8 være svært begrenset. Det fremstår uklart i hvilken grad søk og bruk av informasjonen er betinget av materielle vilkår. I forlengelsen av dette fremstår det uklart hva en eventuell kontroll skal bestå i.

Begrepet «*regelmessig*» er videre vagt og lite forpliktende, og samlet sett gir bestemmelsen etter NIMs syn ikke tilstrekkelige garantier mot misbruk. EOS-utvalget har også uttalt seg med reservasjon for hvilken rolle de skal kunne fylle som sikkerhetsmekanisme etter forslaget, jf. nedenfor under pkt. 4.3.9. NIM ber derfor departementet vurdere om forslaget tilbyr tilstrekkelig sikkerhet mot misbruk. NIM mener også det bør forskriftsfestes hvor ofte registreringene skal gjennomgås, for eksempel to ganger i året.

Det bør også besluttes at loven og praktiseringen av masseinnsamlingen skal evalueres etter en viss tid. Dette vil kunne bidra til å fange opp systematiske feil. Dette sikrer samtidig notoritet og skriftlighet underveis i praktiseringen av loven.

4.3.9. EOS-utvalget og retten til et effektivt rettsmiddel

Etter EMK artikkel 13 har enhver krav på et effektivt rettsmiddel dersom det foreligger mulig krenkelse av EMK. Det er nær sammenheng mellom etterfølgende notifikasjon og tilgang på effektive rettsmidler, ettersom reell tilgang på effektive rettsmidler forutsetter at man har informasjon om at opplysningene er blitt brukt.[31] Når det gjelder hemmelige overvåkingssystemer er det gjerne umulig for en berørt person å kunne benytte et rettsmiddel på egenhånd ettersom det ligger i systemets natur at vedkommende ikke kjenner til overvåkingen. Retten til et effektivt rettsmiddel må i slike tilfeller tolkes i lys av de iboende begrensningene som følger av et slikt system.[32] Blant annet kan uavhengig kontroll på tidspunktet overvåkingen fortsatt er hemmelig, være tilstrekkelig til å ivareta forpliktelsene etter EMK artikkel 13.[33] Retten til et effektivt rettsmiddel er ikke nevnt i høringsnotatet.

Om uavhengig kontroll der en overvåket ikke blir notifisert og dermed ikke selv kan ta skritt for å prøve om overvåkingen er rettmessig, uttaler EMD i *Big Brother Watch* at fullmakter og prosessuelle garantier for overvåkningsorganet er sentralt.[34] Organet bør blant annet ha mulighet til med bindende virkning, å stanse eventuell ulovlig overvåkning og pålegge sletting av slikt materiale.

Lovforslaget åpner ikke for verken innsyn eller notifisering av den som blir rammet av forslaget, verken når innsamlingen skjer, eller senere. NIM legger derfor til grunn at retten til et effektivt rettsmiddel på stadiet der innsamlingen eller behandlingen av opplysningene fortsatt er hemmelig, vil måtte ivaretas av EOS-utvalget. EOS-utvalget skriver i sitt høringssvar til forslaget at

> *«Utvalget har merket seg at høringsnotatet gjennomgående viser til EOS-utvalget som en sikringsmekanisme. Utvalget er ikke ment som en garantist for at feil ikke skjer eller ikke kan skje i EOS-tjenestene. Vår kontroll er stikkprøvebasert og legger ikke opp til en fullstendig gjennomgang av all overvåkingsvirksomhet i PST. Utvalgets eksterne kontroll erstatter ikke den forvaltningsmessige styringen og kontrollen av PST.»* [35]

Departementet bes på denne bakgrunn vurdere hvorvidt EOS-utvalget på dette punkt vil være tilstrekkelig som sikkerhetsmekanisme etter forslaget.

Når det først blir klart at en person har vært gjenstand for overvåking, kreves det etter EMDs praksis at enkeltindivider har et effektivt rettsmiddel for å prøve om overvåkingen

[31] Se bl.a. Szabó og Vissy (37138/14) v. Ungarn avsnitt 57

[32] Klass and Others v. Tyskland (5029/71), avsnittene 68-69.

[33] Se f.eks. om de ulike stadiene ved hemmelig overvåking i Big Brother Watch v. Storbritannia, avsnitt 336.

[34] Se avsnitt 359.

[35] Se EOS-utvalgets høringssvar pkt. 1.

har vært i tråd med konvensjonen.[36] I *Big Brother Watch v. Storbritannia* ble det også vektlagt at det forelå et robust system for å undersøke klager fra individer som *mente* de hadde blitt utsatt for overvåking.[37]

I *Rotaru v. Romania* forelå det krenkelse av artikkel 13 fordi vedkommende som hadde blitt overvåket av etterretningstjenesten ikke hadde hatt et effektivt rettsmiddel for å overprøve hvorvidt lagringen av personopplysninger om ham skulle slettes, eller hvorvidt feilaktige opplysninger skulle rettes.

NIM etterlyser en nærmere vurdering av hvordan retten til et effektivt rettsmiddel skal ivaretas, herunder hvordan ulik rettspraksis fra EMD har overføringsverdi til vår sak, og hvordan retten til et effektivt rettsmiddel skal sikres på de ulike stadiene av prosessen.

I høringsnotatets pkt. 6 legger departementet til grunn at EOS-utvalget kan utføre sin kontrolloppgave innenfor tildelte budsjettrammer. Etter NIMs syn er det sentralt at EOS-utvalget både har rettslig og økonomisk adgang til å føre betryggende kontroll med PSTs bruk av de foreslåtte verktøyene. Dette krever at EOS-utvalget har midler til dette. Hver gang utvalget pålegges en ny oppgave, vil det nødvendigvis innebære at den stikkprøvekontrollen de har ressurser til å gjøre, blir mindre hyppig. På denne bakgrunn etterlyses det en mye mer konkret vurdering av hvorvidt EOS-utvalget har tilstrekkelige ressurser til å kontrollere PSTs behandling etter forslaget, for å sikre en reell og effektiv kontroll.

4.3.10. Oppsummering og helhetsvurdering

Som nevnt foran under pkt. 3.3. må det foretas en helhetlig vurdering av tiltaket for å vurdere om inngrepet vil være forholdsmessig. Dette gjelder uavhengig av om EMDs avgjørelser om bulkinnsamling kommer til anvendelse eller ikke. Forholdsmessighetsvurderingen innebærer at inngrepets art må holdes opp mot formålet inngrepet skal ivareta, og det må vurderes hvilke garantier som foreligger for å forhindre misbruk og formålsutglidning.

Etter NIMs oppfatning er forslaget omfattende og inngripende både på et kollektivt og på et individuelt nivå, slik gjennomgått foran under pkt. 3.2. Dette fordrer gode sikkerhetsmekanismer. Forslaget slik det nå foreligger ledsages ikke av tilstrekkelige sikkerhetsmekanismer, hverken når det gjelder innsamling, behandling og analyse av opplysningene, hva opplysningene kan brukes til, forhåndskontroll eller etterfølgende kontroll. Etter NIMs oppfatning vil forslaget ikke være forholdsmessig slik det nå foreligger, og kan derfor ikke vedtas i en slik form.

[36] Se f.eks. Rotaru v. Romania avsnitt 69.

[37] Se avsnitt 413-415.

5. EMK artikkel 10 og Grunnloven § 100

5.1. Ytringsfrihet og nedkjølende effekt

En ytterligere konsekvens av masseinnsamling av opplysninger på internett er risikoen for en nedkjølende effekt på ytringsfriheten.

Ytringsfriheten er vernet av EMK artikkel 10 og Grunnloven § 100. Innsamling av informasjon vil i utgangspunktet ikke regnes som et inngrep i ytringsfriheten. Forslaget vil imidlertid kunne få virkning på den enkeltes ønske om å ytre seg offentlig i form av en «*chilling effect*».

EMD har i en rekke saker om artikkel 10 vektlagt hvorvidt et tiltak har «*chilling effect*» for samfunnet som helhet, altså hvorvidt tiltaket er egnet til å avskrekke andre fra å ytre seg i fremtiden. Departementet legger i høringsnotatet til grunn at tiltaket kan ha en viss nedkjølende effekt på ytringsfriheten.[38] NIM mener imidlertid at denne effekten er mer alvorlig enn departementet legger til grunn, og derfor fortjener en noe mer utførlig omtale og vurdering enn i høringsnotatet.

Etter NIMs oppfatning vil forslaget kunne innebære en betydelig nedkjølende effekt på personers ønske om å ytre seg. I forbindelse med Teknologirådets rapport fra 2014 ble det gjennomført en undersøkelse hvor nærmere 40 prosent av respondentene oppga at de ville unngått å bruke visse ord og utrykk i sosiale medier som ble overvåket av politiet.[39] Vi viser videre til Datatilsynets personvernundersøkelse av 2019-2020, hvor det blant annet ble avdekket at 16 prosent av befolkningen har unnlatt å delta i kommentarfelt hos en nettavis og Facebook, og ni prosent har unnlatt å søke hjelp/finne informasjon om mental helse, misbruk, avhengighet eller andre sensitive problemer i en søkemotor på nett, fordi de er usikre på om myndigheter slik som politiet og PST kan få tilgang til informasjonen.[40] Den nedkjølende effekten kan særlig tenkes å gjøre seg gjeldende for personer med oppfatninger i ytterkanten av det alminnelige politiske spekteret, ytringer om personlige eller sensitive forhold, eller personer som tilhører grupperinger som kan føle seg i PSTs søkelys, selv om de verken driver med eller planlegger ulovlig virksomhet.

NIM etterlyser en grundigere vurdering av hvordan forslaget vil kunne virke nedkjølende på individers ønske om å ytre seg, særlig på nett, og hvilke samfunnsmessige konsekvenser dette kan få. NIM etterlyser også en grundigere redegjørelse for hvorvidt dette eventuelt vil påvirke samfunnet og demokratiet mer overordnet, og i hvilken grad

[38] Se høringsnotatet s. 14.

[39] Teknologirådet «*På nett med publikum*», 2014, s. 65: https://teknologiradet.no/wp-content/uploads/sites/105/2018/05/Rapport-Paa_nett_med_publikum.pdf

[40] Rapport fra Datatilsynet: https://www.datatilsynet.no/regelverk-og-verktoy/rapporter-og-utredninger/personvernundersokelser/personvernundersokelsen-20192020/

dette avveies mot de formål forslaget søker å oppnå.[41] NIM vil i denne forbindelse minne om at selv muligheten for en tendens i denne retning er ansett som et avgjørende argument i norsk rett. I saken om tilgang til en anonym ytrers IP-adresse uttalte Høyesterett i «runesteinsaken» at hensynet til å oppklare en kriminalsak måtte vike fordi det var «riktig å legge til grunn den mer langsiktige effekten av å skulle gjøre unntak – den såkalte «chilling effect»».[42] Høyesteretts avgjørelse i «Rolfsensaken» viser at hensynet til å unngå en slik «chilling effect» etter omstendighetene også kan veie tyngre enn generelle ønsker om å bekjempe terror, slik at det må foretas en konkret vurdering.[43]

Den lange lagringstiden som er foreslått innebærer også at personer som bekymrer seg for innsamling og lagring ikke bare må bekymre seg for at de kan bli brukt av PST slik deres virksomhet er organisert i dag, men også at fremtidige styresmakter i 15 år fremover vil kunne få tilgang på informasjonen. Frykten for formålsutglidning i hva opplysningene kan brukes til vil i seg selv kunne øke den nedkjølende effekten.

5.2. Kildevern

Det er ikke utenkelig at masseinnsamling av informasjon på internett vil kunne utgjøre et inngrep i kildevernet. Forholdet til pressens kildevern er ikke berørt i høringsnotatet.

Med forbehold om at NIM ikke har informasjon om hvordan det automatiserte analyseverktøyet tenkes brukt, er vår forståelse at KI-systemer med stor informasjonstilgang har kapasitet til å identifisere og gjenkjenne hvem som er avsender av en skjult melding. Dette kan ha en nedkjølende effekt på fremtidige kilder.

Det bør videre foretas en drøftelse av kilders tillit til at de kan ha fortrolig kommunikasjon med journalister. Dette vil gjelde uavhengig av om forslaget direkte rammer kommunikasjon mellom kilder og journalister, ettersom eksistensen av stadig flere tiltak vil kunne etterlate et *inntrykk* av at slik kommunikasjon overvåkes av offentlige myndigheter. Denne ytterligere «nedkjølingseffekten» er noe som bør adresseres eksplisitt. NIM ber departementet vurdere og klargjøre at forslaget tar høyde for pressens kildevern i det videre arbeidet.

6. Avslutning

I et samfunnsperspektiv fordrer et velfungerende demokrati individuell frihet og tillit mellom borgere og stat. Et kontrollsamfunn der staten har tilgang til all informasjon om

[41] Se for eksempel departementets vurdering i Prop.80 L (2019-2020) kap. 11.5.3.4 i forbindelse med ny lov om etterretningstjenesten.

[42] Rt. 2010 s. 1371, avsnitt 62. Se også tilsvarende betraktninger i Standard Verlagsgesellschaft MBH v. Østerrike (nr. 3) (39378/15).

[43] Rt. 2015 s. 1286.

borgerne, vil svekke tilliten og samtidig øke risikoen for myndighetsmisbruk.[44] Dette kan innebære at bruk av automatiserte analyseverktøy for å overvåke åpne kilder ikke bare vil utfordre privatlivet på individnivå, men også på et overordnet kollektivt samfunnsnivå i den grad man søker å innhente og systematisere store mengder informasjon fra befolkningen.

Som det fremgår av gjennomgangen foran, er det NIMs oppfatning at forslaget ikke kan vedtas i den form det nå er fremmet. Vi bistår gjerne i nærmere dialog om hvordan forslaget kan justeres og rammes inn på en måte som bedre ivaretar menneskerettslige krav.

Vennlig hilsen
for Norges institusjon for menneskerettigheter

Adele Matheson Mestad	Mathilde Wilhelmsen	Anders Broderstad
Direktør	Rådgiver	Rådgiver

Dette dokumentet er elektronisk godkjent og har dermed ingen signatur.

[44] NOU 2009:15 s. 51 «Den privates sfære er (...) en forutsetning for menneskets dannelsesprosess og myndiggjøring, samt for demokratiet og maktbalansen».