



POLITIETS
SIKKERHETSTJENESTE

Postboks 4773 Nydalen
0421 OSLO
post@pst.politiet.no
Tlf.nr. 23 30 50 00
Besøksadresse:
Nydalen allé 35

Kommunal- og distriktsdepartementet
Postboks 8112 Dep
0032 OSLO

Kontaktperson:

Deres ref.: 22/6868-1
Vår ref.: 22/05801-2
Dato: 7. februar 2023

NOU 2022:11 Ditt personvern - vårt felles ansvar

Vi viser til høringsbrev av 11. november 2022.

Innledningsvis vil Politiets sikkerhetstjeneste (PST) bemerke at rapporten tar opp temaer tjenesten mener er viktige og forholder seg til i flere sammenhenger, både på et overordnet nivå og i det daglige gjennom PST arbeidsoppgaver. Videre er PST enig i de utfordringene som er påpekt i rapporten hva gjelder hensynet til kriminalitetsbekjempelse på den ene siden og hensynet til personvern på den andre. I en demokratisk rettstat er både sikkerhet og personvern to goder som kan komme i konflikt og som derfor må balanseres på en god måte. Som politi- og sikkerhetstjeneste er det PSTs oppgave å bidra til å sikre at Norge er et trygt land å bo i og PSTs mandat er å forebygge og etterforske de mest alvorlige truslene mot rikets sikkerhet. Dette medfører at PST behandler personopplysninger om norske borgere og har mulighet til å benytte inngripende metodebruk for å skaffe seg tilgang til slike opplysninger. For å kunne gjøre dette er det avgjørende for PST å ha tillitt i befolkningen, noe som forutsetter at tjenesten til enhver tid har et bevisst forhold til personvern og etterlever det regelverket som gjelder for PST.

PST vil hovedsakelig konsentrere seg om merknader til den delen av rapporten som omhandler personvern i justissektoren.

7.1.3 Viktigheten av tillit til justissektoren

Som nevnt innledningsvis og påpekt i rapporten er tillitt i befolkningen avgjørende for at justissektoren, herunder PST, kan utføre arbeidsoppgavene sine. Her vil informasjon og åpenhet om blant annet de vurderinger som tas og metodebruk, stå sentralt.

PST tilstreber å være så åpne som mulige om hvordan tjenesten arbeider. Dette gjelder både gjennom generelle beskrivelser av arbeidsmetoder, men også hvordan PST har håndtert og arbeidet med ulike hendelser. Blant annet gjennom PSTs egen podkast forsøker tjenesten å belyse ulike temaer som er aktuelle innenfor vårt samfunnsoppdrag, herunder om metoder og vurderinger som tas.

Videre har PST i de senere år søkt å utarbeide åpne trusselvurderinger og temarapporter i størst mulig grad, samt å kommunisere ut disse slik at de er mest mulig tilgjengelige for allmennheten. Det er også i PST interesse å kommuniserer ut potensielle trusler slik at bedrifter, virksomheter, miljøer mv. kan melde tilbake til PST om forhold som tjenesten

har behov for i sin oppgaveløsning. Kommunikasjon rundt potensielle trusler medfører også at andre settes i stand til å selv sette inn egne tiltak. PST er helt avhengig av å samarbeide med andre aktører og virksomheter for å forebygge og avverge hendelser som kan true vår sikkerhet. Jo mer komplekst trusselbildet er, jo viktigere er det å samhandle med ulike aktører som viktige komponenter i dette bildet.

Samtidig som det er viktig med åpenhet ligger det i sikkerhets- og etterretningstjenesters natur at man ikke kan gi all informasjon om arbeidsmetoder og vurderinger som tas og det vil heller ikke være innsyn i hvem PST behandler opplysninger om.

Manglende åpenhet her kompenseres til en viss grad ved at regelverket for PSTs behandling av opplysninger er utførlig utformet, noe som skaper klarhet og forutsigbarhet, og at PST kontrolleres av Stortingets kontrollutvalg for etterretnings-, overvåknings- og sikkerhetstjeneste (EOS-utvalget) hva gjelder etterlevelse av PSTs regelverk. I tillegg kommer domstolskontroll hva gjelder tvangsmiddelbruk og tilsyn fra blant annet Justis- og beredskapsdepartementet og Det nasjonale statsadvokatembetet.

Ipsos omdømmeundersøkelse for 2022 viser at PST fortsatt har et godt omdømme i befolkningen, noe PST anser som svært viktig.

7.2.2 Politiregisterloven

Politiregisterloven- og forskriften regulerer som beskrevet i rapporten også PSTs behandling av opplysninger, der PST har særbestemmelser både i loven og forskriften. Blant annet reguleres også PSTs forvaltningsvirksomhet av loven og reglene om informasjonsplikt og innsyn gjelder ikke for PST. PSTs behandling av opplysninger er videre direkte knyttet opp til tjenestens oppgaver gitt i politiloven.

At tjenestens forvaltningsvirksomhet også reguleres av politiregisterloven innebærer at personopplysningsloven kun gjelder for PSTs administrative gjøremål, herunder behandling av opplysninger om PSTs ansatte.

7.3 Utviklingstrekk som påvirker personvernet

Som beskrevet har den gjennomgående digitaliseringen av samfunnet, og den omfattende mengden av data som samles og brukes, hatt stor innvirkning på justissektoren. Dette gjelder både i forhold til nye metoder for politiet å arbeide på, men også at kriminaliteten flytter seg over på digitale flater.

PST ser dette innenfor alle våre arbeidsoppgaver og det er bakgrunnen for at PST de senere årene har etterspurt et regelverk som er oppdatert i forhold til den tiden og det trusselbildet vi lever i for å løse oppgavene våre.

7.3.1 Endringer i kriminalitetsbildet

Det er beskrevet endringer i trusselbildet med bakgrunn i politiets trusselvurdering for 2021, hvor det er pekt på datainnbrudd, spredning av overgrepsmaterialet, løsepengevirus og ekstreme ytringer som noen av de mest alvorlige digitale truslene. I PSTs trusselvurdering for 2022 er det vist til at nettsverksoperasjoner fremdeles vil utgjøre en alvorlig trussel mot Norge, at internett er en stadig viktigere arena for informasjonsinnhenting for fremmede etterretningstjenester og at digitale plattformer fremdeles vil være de viktigste arenaene for radikalisering til høyreekstremisme. Videre at trusselen fra ekstreme islamister primært vil komme fra personer som deltar i ekstreme digitale nettverk.

7.4 Personvernutfordringer i justissektoren

PST er enig i den beskrivelsen som skisseres overordnet om personvernutfordringer i justissektoren. Som nevnt over mener også PST at endringer i kriminalitetsbilde krever nye metoder for at PST skal kunne levere på samfunnsoppdraget sitt. Det er PSTs oppgave å si fra til overordnet myndighet dersom vi ser at vi ikke kan levere på oppgavene som ligger innenfor PSTs mandat på en tilfredsstillende måte eller som det er forventet at PST skal levere på. Dette er bakgrunnen for at PST har fremsatt et behov for nye lovhjemler hva gjelder et tydelig mandat som etterretningstjeneste og utvidet bruk av åpne kilder for dette formålet. Videre har PST kommunisert at arbeidet med å kriminalisere påvirkningsaktivitet bør prioriteres. Som PST har fremhevet i sin årlige trusselvurdering og i andre sammenhenger utgjør uønsket utenlandsk påvirkningsaktivitet en trussel mot nasjonale sikkerhetsinteresser som det er et økende fokus på og forventning om at PST skal håndtere innenfor sin portefølje.

Når det forventes at PST skal levere beslutningsstøtte om ulike forhold PST ikke har hjemmel for behandle opplysninger om og således ikke kan vurdere, må dette kommuniseres videre. Videre prosess og valg av løsninger, herunder eventuelt nye hjemler, der blant annet hensynet til den enkeltes personvern må vurderes, er et rettspolitisk spørsmål som er opp til andre enn PST å vurdere. PST er imidlertid enig i det som er beskrevet under punkt 7.3.3 i rapporten om behovet for nye verktøy og metoder. Vi bemerker at det omtalte lovforslaget til nye hjemler for PST er vesentlig endret etter høringsrunden ved fremleggelse for Stortinget.

7.4.2 Vurdering av personvern i myndighetsutøvelse:

7.4.2.1. Implementering av politidirektivet i politiregisterloven

PST merker seg at kommisjonen skriver at politiregisterloven ikke oppstiller tilstrekkelige konkrete krav og føringer for behandling av personopplysninger, og at den bør forenkles og forbedres.

Etter PSTs vurdering er det mulig loven kunne vært forenklet da regelverket, når man ser politiregisterloven og politiregisterforskriften i sammenheng, kan fremstå komplisert og uoversiktlig. I tillegg kommer for PSTs tilfelle at oppgavene våre og metodebruk er hjemlet i politiloven og straffeprosessloven, som igjen er koblet opp mot bestemmelser i straffeloven og til dels annet regelverk. Tjenesten mener imidlertid at politiregisterforskriften, herunder de særregler som gjelder for PST når det gjelder registrering av personopplysninger, er konkrete og til dels svært detaljerte. En av årsakene til at den delen av politiregisterforskriften som gjelder for PSTs behandling av opplysninger ble endret i 2021, var nettopp at den var svært detaljert utformet.

Når det for øvrig gjelder regler som følger av politidirektivet, men som ikke er inntatt i politiregisterloven, eksempelvis bestemmelser som vil ha betydning for ny teknologi, er PST enig i at det kan være en fordel om disse inntas i regelverket for å unngå uklarheter rundt dette.

7.4.2.5 Deling av opplysninger mellom politiet og andre myndigheter

PST er enig i at tydelige og forutsigbare rammer for informasjonsutveksling er en forutsetning både for godt personvern og for effektiv kriminalitetsbekjempelse.

I mange sammenhenger er PST avhengig av å samhandle med andre offentlige etater for å forebygge kriminalitet. Eksempelvis ser vi at samhandling mellom helsevesenet og politiet/PST kan være avgjørende for å sørge for at personer som kan falle inn under begges mandat fanges opp før de begår alvorlige voldshandlinger. PST har forståelse for

det tillitsforholdet som må være mellom helsevesenet og den enkelte, men ser at også her er det en balanse mellom personvern og kriminalitetsbekjempelse som må vektas. Fra PSTs ståsted erfarer vi i samhandling med helsevesenet at det kan oppstå enkelte utfordringer knyttet til utlevering av opplysninger. Politiet/PST har nokså vide hjemler til å dele opplysninger med andre etater etter politiregisterloven § 30 og i politiregisterforskriften § 9-6, hvor utlevering til helsemyndighetene er særskilt nevnt. Utfordringene med å motta informasjon fra helsevesenet knytter seg ikke nødvendigvis til manglende bestemmelser i regelverket, men kan ofte knyttes til usikkerhet til praktisering av gjeldene regelverk. Grensesnittet mellom taushetsplikten og det som omfattes av varslingsplikten og opplysningsretten og definisjonen av hva som ligger i «tungtveiende offentlige interesser og fare for liv og helse» i helsepersonelloven §§ 23 og 31 er uklare. I tillegg kommer at journalføringsplikten i pasientjournalforskriften § 14 i mange tilfeller medfører at PST ikke kan be om eller utlevere informasjon dersom det fremkommer av journalen, som den enkelte har innsyn i.

Det er videre beskrevet i rapporten at det ofte er politiske forventninger til og gode intensjoner om bredere samarbeid på tvers av ulike etater, uten at de rettslige rammene alltid er like klare. PST erfarer også dette, særlig ved etablering av felles sentre der ulike etater skal samarbeide. Selv om hver etat har mulighet til å dele opplysninger og arbeide på eget mandat, vil det oppstå utfordringer knyttet til behandlingsansvar for den totale mengden opplysninger, ulike oppgaveporteføljer for den enkelte tjeneste som styrer hvilke opplysninger som kan behandles og hvilke flater man skal samarbeide på. Dette kunne etter PSTs syn med fordel vært regulert, men vi ser at det kan være utfordrende å utforme en generell regel om dette.

7.4.4 Effektiv domstolskontroll

Under punktet er det blant annet vist til straffeprosessloven § 170a om at et tvangsmiddel ikke kan brukes dersom det fremstår som et uforholdsmessig inngrep. Kommisjonen peker på at flere mindre inngripende tiltak kan ha en samlet effekt som utgjør et større inngrep i personvernet. På bakgrunn av dette mener kommisjonen at det bør inntas et tillegg i straffeprosessloven § 170a som sikrer at det gjøres en vurdering av den samlede bruken av ulike etterforskningsmetoder ikke blir et uforholdsmessig inngrep. Og videre at det i et slikt tillegg understrekes at hensynet til personvern skal vektlegges i vurderingen.

Etter PSTs vurdering og erfaring tas det allerede i dag hensyn til den samlede bruken av ulike tvangsmidler ved vurderingen av inngrepet og der man søker å bruke de mindre inngripende metodene først. Dette kommer eksempelvis til uttrykk i Riksadvokatens rundskriv RA-2018-2 om infiltrasjon og provokasjon som etterforskningsmetode der det fremgår at det ved forholdsmessighetsvurderingen må tas hensyn til det samlede overvåkingstrykk som den mistenkte har vært, og kommer til å bli, utsatt for. Også politiloven § 6 annet ledd gir anvisning på en forholdsmessighetsvurdering av inngrepet og at svakere midler må være prøvd ut før sterkere midler tas i bruk.

Videre mener PST at det i de forholdsmessighetsvurderingene som skal foretas nettopp ligger et krav om å hensynta personvernet til den enkelte ved vurderingen av hvor inngripende tvangsmiddelet er.

7.4.7 Systemer og verktøy for å ivareta personvernet

7.4.7.1 Håndtering av digitale beslag og overskuddsinformasjon

det tillitsforholdet som må være mellom helsevesenet og den enkelte, men ser at også her er det en balanse mellom personvern og kriminalitetsbekjempelse som må vektas. Fra PSTs ståsted erfarer vi i samhandling med helsevesenet at det kan oppstå enkelte utfordringer knyttet til utlevering av opplysninger. Politiet/PST har nokså vide hjemler til å dele opplysninger med andre etater etter politiregisterloven § 30 og i politiregisterforskriften § 9-6, hvor utlevering til helsemyndighetene er særskilt nevnt. Utfordringene med å motta informasjon fra helsevesenet knytter seg ikke nødvendigvis til manglende bestemmelser i regelverket, men kan ofte knyttes til usikkerhet til praktisering av gjeldene regelverk. Grensesnittet mellom taushetsplikten og det som omfattes av varslingsplikten og opplysningsretten og definisjonen av hva som ligger i «tungtveiende offentlige interesser og fare for liv og helse» i helsepersonelloven §§ 23 og 31 er uklare. I tillegg kommer at journalføringsplikten i pasientjournalforskriften § 14 i mange tilfeller medfører at PST ikke kan be om eller utlevere informasjon dersom det fremkommer av journalen, som den enkelte har innsyn i.

Det er videre beskrevet i rapporten at det ofte er politiske forventninger til og gode intensjoner om bredere samarbeid på tvers av ulike etater, uten at de rettslige rammene alltid er like klare. PST erfarer også dette, særlig ved etablering av felles sentre der ulike etater skal samarbeide. Selv om hver etat har mulighet til å dele opplysninger og arbeide på eget mandat, vil det oppstå utfordringer knyttet til behandlingsansvar for den totale mengden opplysninger, ulike oppgaveporteføljer for den enkelte tjeneste som styrer hvilke opplysninger som kan behandles og hvilke flater man skal samarbeide på. Dette kunne etter PSTs syn med fordel vært regulert, men vi ser at det kan være utfordrende å utforme en generell regel om dette.

7.4.4 Effektiv domstolskontroll

Under punktet er det blant annet vist til straffeprosessloven § 170a om at et tvangsmiddel ikke kan brukes dersom det fremstår som et uforholdsmessig inngrep. Kommisjonen peker på at flere mindre inngripende tiltak kan ha en samlet effekt som utgjør et større inngrep i personvernet. På bakgrunn av dette mener kommisjonen at det bør inntas et tillegg i straffeprosessloven § 170a som sikrer at det gjøres en vurdering av den samlede bruken av ulike etterforskningsmetoder ikke blir et uforholdsmessig inngrep. Og videre at det i et slikt tillegg understrekes at hensynet til personvern skal vektlegges i vurderingen.

Etter PSTs vurdering og erfaring tas det allerede i dag hensyn til den samlede bruken av ulike tvangsmidler ved vurderingen av inngrepet og der man søker å bruke de mindre inngripende metodene først. Dette kommer eksempelvis til uttrykk i Riksadvokatens rundskriv RA-2018-2 om infiltrasjon og provokasjon som etterforskningsmetode der det fremgår at det ved forholdsmessighetsvurderingen må tas hensyn til det samlede overvåkingstrykk som den mistenkte har vært, og kommer til å bli, utsatt for. Også politiloven § 6 annet ledd gir anvisning på en forholdsmessighetsvurdering av inngrepet og at svakere midler må være prøvd ut før sterkere midler tas i bruk.

Videre mener PST at det i de forholdsmessighetsvurderingene som skal foretas nettopp ligger et krav om å hensynta personvernet til den enkelte ved vurderingen av hvor inngripende tvangsmiddelet er.

7.4.7 Systemer og verktøy for å ivareta personvernet

7.4.7.1 Håndtering av digitale beslag og overskuddsinformasjon

Som kjent ble Norge dømt i Den europeiske menneskerettighetsdomstolen (EMD) for krenkelse av EMK artikkel 8 i forbindelse med beslag av mobiltelefonen til en siktet. Avgjørelsen fra EMD medførte at riksadvokaten ved direktiv av 9. juni 2021 innførte et system der en egen teknisk enhet, organisatorisk atskilt fra etterforskningsenheten, har ansvar for å gjennomgå digitale enheter i forbindelse med beslag for å hindre at etterforskere får innsyn i opplysninger det er forbudt å beslaglegge etter straffeprosessloven § 119.

Herværende rapport er utferdiget før Høyesteretts kjennelse av 30. juni 2022 som sier at den ordningen det er lagt opp til i riksadvokatens direktiv, er tilstrekkelig for å sikre EMKs krav til klare og prosessuelle garantier ved utsortering av taushetsbelagt materiale. PST forholder seg således til direktivet.

7.4.8 Tilsyn og kontroll med behandlingen av personopplysninger

Det er EOS-utvalget (Stortingets kontrollutvalg for de hemmelige tjenestene) som fører tilsyn med tjenesten. Dette gjøres ved flere inspeksjoner årlig, både ved PSTs hovedkontor i Nydalen og ved PST-enhetene i politidistriktene. I tillegg til stedlig kontroll, kontrolleres tjenesten gjennom skriftlige spørsmål både om generelle forhold ved tjenesten eller om registrering av enkeltpersoner som tas opp av utvalget på eget initiativ og ved spørsmål om registrering av enkeltpersoner etter henvendelse fra disse til EOS-utvalget. Antallet klagesaker og inspeksjoner hvert år, samt funn ved disse, fremgår av årsmeldingene til EOS-utvalget. I 2021 hadde EOS-utvalget seks stedlige inspeksjoner ved PST. Utvalget og sekretariatet har tilgang til alle tjenestens systemer for kontroll av at opplysninger der behandles i henhold til regelverket.

Etter PSTs vurdering sikrer den hyppige kontrollen av tjenesten at bevissthet rundt etterlevelse av regelverket hele tiden er tilstede og at internkontrollen i tjenesten også har stort fokus.

Annet:

Når det gjelder utviklingen i det teknologiske landskapet som er beskrevet i kapittel 5 er PST enig i beskrivelsen av at digitaliseringen av samfunnet har ført til betydelige endringer i samfunnsikkerhetsbildet på tvers av landegrensene og nasjonalt. Informasjonen som samles inn og analyseres av forskjellige aktører bidrar til et bredt og uoversiktlig trusselbilde for både myndigheter og virksomheter. Som sikkerhetsmyndighet skaper dette også utfordringer for PST og fordrer at tjenesten er nødt til å ha verktøy for å være tilstede der truslene utspiller seg. PST er imidlertid enig i at inngripende teknologi ikke gjøres uten å ha kartlagt hvilke problemer man faktisk søker å løse og at det gjøres grundige vurderinger av om det finnes mindre inngripende veier til målet. Videre er det viktig med en offentlig debatt rundt disse spørsmålene.

For øvrig er PST enig i mange av de anbefalingene Personvernkommissjonen har fremlagt i sin rapport og mener at hensynet til sikkerhet og kriminalitetsbekjempelse også er godt balansert og beskrevet i rapporten.


Beate Gangås