Datatilsynet

JUSTIS- OG BEREDSKAPSDEPARTEMENTET
Postboks 8005 Dep.
0030 OSLO

Deres referanse	Vår referanse	Dato
21/4559 - NNO	21/03329-2	05.01.2022

Høringsuttalelse - PSTs etterretningsoppdrag og bruk av åpent tilgjengelig informasjon

Datatilsynet viser til høringsbrev av 7. oktober 2021 fra Justis- og beredskapsdepartementet. om forslag om endringer i politiloven, politiregisterloven og politiregisterforskriften mv. og PSTs etterretningsoppdrag og bruk av åpent tilgjengelig informasjon

Forslagene i dette høringsnotatet gjelder innhenting og behandling av informasjon fra åpne kilder, eksempelvis internett, avisartikler og åpne registre, til bruk for etterretningsformål, herunder beskrivelse av fenomener, trender og utvikling.

Ifølge høringsnotatet så vil det kunne innhentes opplysninger om «en stor andel av befolkningen». Det omtales også som «ubegrenset nedlasting av opplysninger fra åpne kilder». Opplysningene kan lagres i 15 år.

Opplysningene kan brukes til PSTs etterretningsvirksomhet som å kartlegge trender og utviklingstrekk og utarbeide analyser og etterretningsvurderinger.

Søk mot enkeltpersoner og bruk skal etter forslaget kunne gjøres i opprettelse av eller i forebyggende sak og til etterforskning av saker som faller inn under PSTs ansvarsområde. Forslaget gir mulighet til slik bruk uten uavhengig forhåndskontroll.

Oppsummering av Datatilsynets vurderinger

Forslaget berører sentrale spørsmål knyttet til personvern, ytringsfrihet og sikkerhet som krever en grundig utredning og avveining. Internett er kanskje den viktigste kanalen for utveksling av tanker, meninger og en arena hvor vi organiserer våre liv i grupper, organisasjoner og sosiale medier.

Enhver overvåking innebærer et inngrep i denne friheten som vil få konsekvenser for hvordan den utøves og hvordan vårt demokratiske samfunn fungerer. Forslaget må sees i sammenheng

med andre større overvåkingstiltak som politi og etterretningstjenesten har fått hjemmel til å innføre. Dette dreier seg om tilrettelagt innhenting som vil lagre metadata om internettbruk, lagring av ip-adresser og overvåking av flypassasjerer. Samlet sett innebærer dette at myndighetenes mulighet til å overvåke borgerne har blitt betydelig utvidet de siste årene.

Datatilsynet ser at PST har et behov for å følge med og etterforske på internett, men på grunn av det betydelige overvåkingspotensialet som digital overvåking med de muligheter kunstig intelligens og andre stordataverktøy åpner for, så må denne aktiviteten foregå under streng kontroll og rammer for den enkeltes rettsikkerhet.

Forslaget medfører en betydelig risiko for å samle inn taushetsbelagt informasjon som ufrivillig har bli lagt ut på både internett og darknet, feilaktig eller utdatert informasjon tatt ut av kontekst og opplysninger som blir utilgjengelig ved at de blir slettet fra internett etter innsamling. Alt dette medfører en risiko for analyseverktøy basert på kunstig intelligens eller andre liknende metoder vil gjøre feil basert på kvaliteten av den innsamlede informasjonen.

Datatilsynet mener at konsekvensene av forslaget kan bli for store og at det derfor ikke bør innføres i sin nåværende form.

Forslaget mangler en grundig vurdering av konsekvenser for personvern og ytringsfrihet, og er ikke i samsvar med praksis fra EMD og Europadomstolen når det gjelder masseinnsamling av personopplysninger til bruk for etterretnings- og politiformål.

Et endret forslag må være i samsvar med de kravene til ende til ende-kontroll som følger av blant annet *Big Brother Watch and Others mot Storbritannia og Center för Rättvisa mot Sverige*, samt praksis fra Eu-domstolen blant annet *La Quadrature du Net and Others (sak C-511/18).*

Disse dommene inneholder konkrete krav til hvordan denne type overvåkingssystemer bør innrettes og kontrolleres for å være i samsvar med menneskerettighetene.

Våre innspill til forslaget kan kort oppsummeres til:

- Målrettet innhenting som er underlagt uavhengig forhåndskontroll
- En klarere definisjon av hva som innhentes og hvem som rammes
- En drøftelse av PSTs metodebruk og behovet for domstolskontroll
- En betydelig kortere lagringstid.

Betydningen av personvern og mulige konsekvenser av overvåking

Retten til privatliv, ytringsfrihet og personvern er grunnleggende verdier som er nødvendige forutsetninger for et demokratisk samfunn.

Personvern handler om ivaretagelse av den personlige integritet, herunder mulighet for

privatliv, selvbestemmelse og selvutfoldelse. Personvern og retten til privatliv er rettigheter som blant annet begrenser offentlige myndigheters mulighet til å innhente og lagre visse former for informasjon om sine borgere.

For store inngrep i personvernet og privatlivet vil gjøre det vanskelig for det enkelte menneske å skape seg et rom til å utvikle refleksjoner og vurderinger på et selvstendig grunnlag, uten å bli forstyrret eller kontrollert av andre.

Den enkelte vil kunne oppleve et inngrep fra myndighetene i den private sfære som en svekkelse i maktbalansen mellom en selv som individ og omgivelsene. «Kunnskap er makt» er et allment akseptert uttrykk i samfunnsforskningen for å forstå maktforholdet mellom staten og borgerne. Det at staten har kunnskap om sine borgere kan virke disiplinerende i negativ retning og innebære at borgerne avstår fra lovlige aktiviteter de normalt ville ha foretatt seg.

Et tiltak hvor store deler av borgernes kommunikasjon er gjenstand for lagring og søk innebærer at borgeren aldri fullt ut kjenner sitt publikum. Dette synet henter blant annet støtte fra sosiologiske teorier som sier at menneskers kommunikasjon med hverandre er kontekstuell, det vil si at hvem budskapet er ment for er avgjørende for form og innhold. Mennesker måler sitt publikum og tilpasser budskapet etter hvem som lytter. En utenforstående og potensiell "medlytter" endrer samhandlingens forutsetninger, også selv om samtalepartene "ikke har noe å skjule".

Meningsdannelse skjer ikke bare i den offentlige debatt, den skjer også i den private sfære.

Den private sfære er derfor en viktig ressurs i et fungerende demokrati. Drøftelser rundt middagsbordet, mellom venner, kollegaer, studenter og i foreninger er med å forme den enkeltes politiske forståelse og engasjement. Ettersom stadig mer av samhandlingen i den private sfære flyttes over på elektroniske møteplasser, er det viktigere å verne om privatlivet i slike sammenhenger. Deler av internett vil derfor kunne defineres som en mellomting mellom offentlige og private rom.

Den private sfære er ofte et arnested for kritiske tanker, utvikling av holdninger og perspektiver som kan utfordre hva som der og da er alminnelig akseptert - på godt og vondt.

Om usikkerhet eller frykt for å bli overvåket påvirker hva som kommuniseres, vedrører det vilkårene for meningsdannelse i den private sfære. Overvåking av privat kommunikasjon er derfor ikke bare et spørsmål om personvern i snever forstand, som avgrenset til integritetskrenkelse på et individnivå. Det er også et spørsmål om maktforholdet mellom innbygger og stat, og om vilkårene for utvikling av normer og perspektiver som utfordrer det bestående i et demokrati. Frykten er at overvåkingstiltak kan legge en demper på noe som i ettertid viser seg å være viktig for samfunnets utvikling.

Vi lever våre liv på internett, og overvåking av internett vil kunne medføre at vi unngår å søke kunnskap eller delta i fellesskap fordi vi er usikre på hvordan vi blir oppfattet. Dette kan

påvirke vår mulighet til å utvikle oss og kan begrense vår utfoldelse.

Overvåking vil for de fleste gi en følelse av ubehag. Dette kan begrense muligheten til å danne forhold til andre personer gjennom fortrolighet, samt at det gjør det vanskeligere å utvikle oss som autonome individer. En forutsetning er at samfunnet gir rom og plass for at man kan velge å trekke seg tilbake og føle seg fri fra andres blikk.

Andre konsekvenser

Overvåking skaper risiko for diskriminering ved at automatiske analyseverktøy kan inneholde algoritmeskjevheter (bias) som gjør at enkelte grupper rammes sterkere enn andre.

Dette kan igjen medføre en nedkjølingseffekt og konsekvenser for ytringsfriheten ved at den enkelte unnlater å ytre seg når de vet at myndighetene følger med.

I Datatilsynets personvernundersøkelse 2019/2020 svarer 16% at de har unnlatt å delta i en debatt i kommentarfelt eller på Facebook fordi de er usikre på om myndigheter slik som politiet, PST eller etterretningstjenesten, kan få tilgang til informasjonen. Dette er et oppsiktsvekkende høyt tall i et land hvor tilliten til offentlige myndigheter generelt sett er høy.

Overvåkingstiltak kan også medføre konsekvenser for organisasjonsfriheten ved at den enkelte unnlater å melde seg inn i organisasjoner og grupper når aktiviteten kan bli overvåket.

Også forsamlingsfriheten kan bli berørt ved at arrangører og deltakere i demonstrasjoner kan unnlate å benytte seg av sosiale medier som verktøy for å organisere lovlige demonstrasjoner.

Metoder for innsamling og bruk av informasjon

Slik systemet er beskrevet så vil det samle inn åpent tilgjengelig informasjon som nettavisartikler, åpne offentlige registre, åpne diskusjoner i sosiale medier, kommentarfelt, blogger mv. Informasjonen skal lagres i 15 år.

Ifølge høringsnotatet så vil det kunne innhentes opplysninger om «om en stor andel av befolkningen». Det omtales også som «ubegrenset nedlasting av opplysninger fra åpne kilder»

Opplysninger som behandles etter ny politiregisterlov § 65 a kan opplysningene brukes til følgende formål:

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

Datatilsynet vil påpeke at dette er stort sett hele PSTs virksomhetsområde og ikke begrenset til etterretningsformål noe som i betydelig grad utvider personvernkonsekvensene da søk kan bli rettet mot enkeltpersoner.

Systemet vil benytte to typer verktøy; automatiserte analyseverktøy og søk.

I høringsnotatet s. 23 går det frem at automatiserte analyseverktøy jf. politiregisterforskriften ny § 21-8 annet ledd bare skal brukes til etterretningsformål:

> «Eventuelle automatiserte analyseverktøy må innrettes slik at disse brukes til etterretningsformål, det vil si for å kartlegge trender og utviklingstrekk innenfor PSTs ansvarsområde, og i denne forbindelse utarbeide analyser og etterretningsvurderinger. Bruk av automatiserte analyseverktøy kan dermed ikke skje med det formål å kartlegge enkeltindividers aktivitet på nett.»

Imidlertid sies det også på s. 26 i høringsnotatet:

> «Dette innebærer eksempelvis at dersom PST, når de bruker opplysninger for etterretningsformål, kommer over opplysninger om en person som det er grunn til å undersøke om forbereder et straffbart forhold som PST skal forebygge, vil de kunne registrere denne personen i sine alminnelige registre»

Dette innebærer at de automatiske analyseverktøyene vil kunne resultere i treff som berører enkeltpersoner.

Verktøyene er i liten grad er beskrevet i høringsnotatet. Det er derfor vanskelig å si hvor grensen for de ulike søke og analyseverktøyene går.

Datatilsynet vil bemerke på generelt grunnlag at utvikling av kunstig intelligens har åpnet for nye muligheter for søk. Det er som eksempel mulig å kartlegge relasjoner gjennom lenkeanalyse, tilordne en mening eller holdning til innlegg på sosiale medier ved hjelp av naturlig språkprosessering og sentimentanalyse. Maskinlæring gjør det mulig å finne mønstre som kan være vanskelige å se for mennesker, mens dype nevrale nettverk kan identifisere og foreslå helt nye kategorier av mønstre for videre undersøkelse.

Det fremstår som uklart om PSTs behandling innebærer profilering jf. personvernforordningen art. 4 nr. 4. I personvernforordningen er det fastsatt egne regler i art. 2 for å ivareta de registrertes rettigheter som bli gjenstand for profilering.

I forbindelse med gjennomføringen av politidirektivet direktiv (EU) 2016/680 som ligger til grunn for politiregisterloven ble ikke direktivets art. 11 som omhandler automatiske beslutningsprosesser og profilering gjennomført. Politiregisterloven mangler derfor den sentrale bestemmelsen for å sikre de registrertes rettigheter på dette området. Bestemmelsen inneholder blant annet et forbud mot profilering som fører til diskriminering av fysiske personer basert på særlige kategorier personopplysninger, samt plikt til å innført egnede tiltak for å verne den registrertes rettigheter, friheter og berettigede interesser.

Denne type behandling er særlig vektlagt som risikofylt i fortalepunkt 50:

> «når behandlingen gjelder personopplysninger som avslører rasemessig eller etnisk opprinnelse, politisk oppfatning, religiøs eller filosofisk overbevisning, fagforeningsmedlemskap, og behandling av genetiske eller biometriske opplysninger som entydig kan identifisere en person, helseopplysninger, seksuelle forhold eller straffedommer og straffbare forhold eller tilknyttede sikkerhetstiltak, når personlige aspekter vurderes, særlig for å analysere og forutsi aspekter som gjelder arbeidsprestasjoner, økonomisk situasjon, helse, personlige preferanser eller interesser, pålitelighet eller atferd, plassering eller bevegelser, for å opprette eller bruke personlige profiler, når sårbare fysiske personers, særlig barns, personopplysninger behandles, eller når behandlingen omfatter en stor mengde personopplysninger og berører et stort antall registrerte».

Høringsnotatet behandler ikke hvordan den forslåtte behandlingen skal reguleres slik at den blir i samsvar med politidirektivet og de generelle prinsippene knyttet til profilering i personvernforordningen.

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

Datatilsynet mener at innhentingsmetode burde vært drøftet i høringsnotatet.

Om «åpent tilgjengelig informasjon»

I høringsnotatet understrekes det at forslaget er begrenset til åpent tilgjengelig informasjon.

Med åpent tilgjengelig informasjon menes i høringsnotatet informasjon som er allment tilgjengelig for offentligheten, i hovedsak i det digitale rom. Det er ikke avgjørende hvor eller på hvilken måte informasjonen er gjort åpent tilgjengelig. Åpent tilgjengelig informasjon omfatter for eksempel nettavisartikler, åpne offentlige registre, åpne diskusjoner i sosiale medier, kommentarfelt, blogger mv.

Forslaget skal ikke omfatte informasjon publisert på lukkede nettsteder eller private samtaler på chattetjenester, eposter eller annen kryptert eller privat kommunikasjon.

Hvorvidt et nettsted kan anses som offentlig tilgjengelig, vil bero på om og i hvilken grad det utøves en reell kontroll med tilgangen til nettstedet. Informasjon regnes derfor som åpen selv om det kreves et abonnement eller registrering for å få tilgang, for eksempel et abonnement på en nettavis eller at det må opprettes en bruker på sosiale medier. Når det gjelder data fra sosiale medier, vil dette være offentlig tilgjengelig data som brukere frivillig har lagt ut.

Det fremstår som om høringsforslaget hviler på en antakelse om at informasjonen som finnes på internett i hovedsak/ofte er selvpublisert. Med andre ord at informasjonen kan knyttes til brukeren som poster informasjonen - for eksempel ved at det gjenspeiler deres meninger e.l. Det fremgår forutsetningsvis av begrunnelsen for å hindre innsyn:

> *«I tillegg vil merverdien av innsyn være begrenset, all den tid den enkelte fritt kan søke opp informasjon som er publisert på internett om en selv».*

Datatilsynet vil bemerke at internett ikke alltid fungerer på denne måten. Falske kontoer kan opprettes. Beskyldninger og karakteristikker om andre brukere hagler i kommentarfeltet. Intim og personlig informasjon kan bli ulovlig tilgjengeliggjort, og brukere kan bli «doxxet» mot sin vilje – det vil si at personopplysninger blir samlet inn og publisert for å ramme enkeltpersoner.

I høringsnotatet åpnes det også for innsamling av opplysninger fra «det mørke nettet»

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

Selv om deler av «det mørke nettet» er kryptert og krever ulike typer autorisasjon for å få tilgang til informasjon og nettsteder, brukes det også til å fritt utveksle opplysninger til bruk for eksmpelvis hackere eller publisering etter løsepengeangrep hvor løsepenger ikke ble betalt.

Blant annet ble opplysninger om over 475 000 norske Facebook-brukere lekket etter et datainnbrudd. Et nærliggende eksempel vil også være datainnbruddet mot Østre Toten kommune hvor dokumenter med opplysninger om innbyggerne ble lekket på det mørke nettet, blant annet taushetsbelagt informasjon.

Ved større og flere lekkasjer, med tilsvarende lang lagringstid, kan det i realiteten bli langt mer informasjon om enkeltpersoner enn hva som postes online og er søkbart gjennom tradisjonelle søkemotorer.

En udifferensiert og vilkårlig innsamling over 15 år, slik det er foreslått i høringsnotatet, vil kunne innebære at PST vil lagre også store mengder taushetsbelagt informasjon og særlige kategorier som de ikke ville ha lov til å innhente på annen måte. Det er særlig tidsperspektivet og mangelen på målretting som er avgjørende her.

I forslaget er dette formulert som:

> § 65 a Behandling av åpent tilgjengelig informasjon til etterretningsformål
>
> Politiets sikkerhetstjeneste kan behandle åpent tilgjengelig informasjon for etterretningsformål, jf. § 64 tredje ledd nr. 6, uten at bestemmelsene i §§ 6 og 7

> kommer til anvendelse. Informasjon er ikke åpent tilgjengelig dersom tilgang krever forsering av passord eller lignende beskyttelsesmekanismer.

Det er vist til at det i etterretningstjenesteloven § 6-2 er det inntatt en negativ avgrensning, ved at det er angitt at informasjon ikke er åpent tilgjengelig dersom «tilgang til informasjonen krever aktiv fordekt opptreden eller forsering av passord eller andre lignende beskyttelsesmekanismer».

Datatilsynet registrerer at begrensningen om «aktiv fordekt opptreden» ikke er tatt med. Dette er relevant for forståelsen av hva forslaget definerer som et offentlig tilgjengelig nettsted. I forslaget er det lagt til grunn at:

> «Informasjon regnes derfor som åpen selv om det kreves et abonnement eller registrering for å få tilgang, for eksempel et abonnement på en nettavis eller at det må opprettes en bruker på sosiale medier.»

Dette er behandlet i forarbeidene til etterretningstjenesteloven Prop. 80 L (2019–2020), merknader til de enkelte bestemmelsene kap 17 § 6-2:

> «Andre punktum fastsetter i hvilke tilfeller informasjon ikke regnes som åpent tilgjengelig. For det første regnes informasjon ikke som åpent tilgjengelig hvis tilgang til den krever aktiv fordekt opptreden, for eksempel ved at en tjenesteperson utgir seg for å være en annen, ikke-fiktiv person og gjennom samhandling med mennesker oppnår tilgang til for eksempel et forum på Internett. I så fall vil det være menneskebasert innhenting etter § 6-3.
>
> Det regnes derimot ikke som aktiv fordekt opptreden hvis Etterretningstjenesten, gjennom en fiktiv bruker, opptrer med normal aktivitet for å få eller opprettholde tilgang til for eksempel et forum eller gruppe på et nettsamfunn. Hvis slik aktivitet antar karakter av manipulasjon, vil det derimot være menneskebasert innhenting etter § 6-3. Det er ikke aktiv fordekt opptreden å betale vederlag for tilgang til informasjon som tilbys til allmennheten.»

Dette reiser spørsmål om PSTs metodebruk og kontrollen av denne. Det er uklart om når departementet åpner for at det «opprettes en bruker på sosiale medier» - og om brukeren vil tilkjennegi at det er en bruker disponert av PST.

Det er grunn til å problematisere at atferd som bryter med retningslinjene til de store plattformtjenestene som Facebook når det gjelder fiktive brukere, skal lovfestes og benyttes uten en streng kontroll. Spørsmålet er om det er ønskelig med en offentlighet der hvor politimyndigheter og etterretningstjenester kan registrere og overvåke det som ytres basert på handlinger som i seg selv ikke er tillatt av de enkelte tjenestene.

Facebook har blant annet beskrevet hvordan de mener politimyndigheters bruk av fiktive kontoer og overvåkningssystemer strider mot deres retningslinjer. Se for eksempel BBC News - Facebook tells LA police to stop spying on users with fake accounts.

Som en del av et mulig automatisert overvåkingssystem, så åpner bruken av fiktive brukeridentiteter for svært store muligheter for overvåking av internett, uten at dette er drøftet i høringsnotatet.

Datatilsynet savner en prinsipiell vurdering av hva som er å anse som åpent tilgjengelig.

Vurderingen bør ta utgangspunkt i behovet for vern av ytringsfrihet og privatliv, veid opp mot myndighetenes behov for overvåking av elementer som kan anses som en trussel mot samfunnet. Det kan argumenteres for at ytringer på internett må vurderes i lys av hvor de er ytret. Sosiale medier ivaretar forskjellige funksjoner, som ytringer som helt klart er ment for offentligheten, mens det andre steder bærer preg av private ytringer mellom få personer. Dette skillet blir viktig fordi utgangspunktet er at en ikke skal bli overvåket, og det at en ytrer seg gir ikke nødvendigvis et klarsignal til å bli registrert.

I stedet for en tilnærming hvor alt anses åpent tilgjengelig dersom ikke brukerne selv aktivt har tatt grep for å beskytte opplysningene, så kan definisjonen ta utgangspunkt i en generell vurdering av hva som er ytret i det offentlige rom.

Som eksempel nevner vi straffeloven § 10 som sier noe om offentlig sted og offentlig handling.

> «Med offentlig sted menes et sted bestemt for alminnelig ferdsel eller et sted der allmennheten ferdes.
>
> En handling er offentlig når den er foretatt i nærvær av et større antall personer, eller når den lett kunne iakttas og er iakttatt fra et offentlig sted. Består handlingen i fremsettelse av en ytring, er handlingen også offentlig når ytringen er fremsatt på en måte som gjør den egnet til å nå et større antall personer.»

I forarbeidene Ot.prp. 90 (2003-2004) pkt. 12.2.2 er det uttalt:

> «Det andre alternativet er at handlingen er foretatt i overvær av et større antall personer. Etter rettspraksis vil dette si ca 20-30 personer. Om det skjer på privat område og bare særskilt utvalgte slipper inn, er ikke avgjørende når antallet blir så høyt som nevnt.»

I Rt. 2020 s.184 er det uttalt:

> «21) Jeg konstaterer først at det ikke har selvstendig betydning for bedømmelsen av ytringens straffbarhet at den er fremsatt på Facebook. Vilkåret er at ytringen er fremsatt «offentlig», som er definert nærmere i straffeloven § 10. En Facebook-gruppe med omkring 20 000 medlemmer, slik tilfellet var her, oppfyller utvilsomt denne definisjonen, selv om gruppen var lukket. Dette har ikke vært omtvistet."

Borgernes forventning om å kunne ytre seg fritt utenfor myndighetenes kontroll, vil trolig være større i mindre fora, en i grupper eller steder som når ut til en større krets.

Datatilsynet vil påpeke at uavhengig av denne definisjonen, så vil en omfattende registrering av ytringer fremsatt i det offentlige rom kunne ha negative konsekvenser.

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

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

EMK

Retten til privatliv er en grunnleggende forutsetning for et fritt demokratisk samfunn. Rettigheten er nedfelt i Grunnloven § 102, EMK art. 8 og FNs internasjonale konvensjon om sivile og politiske rettigheter (SP) art. 17.

Staten må vurdere om tiltaket vil medføre et inngrep, og i så fall om inngrepet er i samsvar med loven, og om det er nødvendig i et demokratisk samfunn.

Helt sentralt står lovskravet som krever at inngrepet i retten til respekt for privatliv må være hjemlet i nasjonal lov. Lovskravet innebærer ikke bare at det skal foreligge en nasjonal lov som regulerer inngrepet, men innebærer også et kvalitetskrav til loven: lovgivningen må være tilstrekkelig klar og forutberegnelig.

Dette kravet har som formål å verne mot vilkårlige inngrep fra myndighetene. Jo større inngrepet er, jo strengere må kravet tolkes. Loven må altså være klar og forståelig nok slik at den gjengse borger, om enn med rådgivning, kan forutse sin rettsposisjon.

Et inngrep må også forfølge legitime formål og være nødvendig i et demokratisk samfunn.

Bestemmelsen krever at det må foretas en avveining mellom samfunnets/statens interesse og inngrepet i retten til privatliv. Det må derfor vurderes både fordeler og ulemper ved tiltaket. Dette for å fastslå om inngrepet i privatlivet er forholdsmessig.

I dette ligger et krav om å vurdere hvorvidt den skaden som er gjort ved inngrepet er begrenset ved egnede tiltak som reduserer virkningen av skaden.

I denne sammenhengen betyr dette blant annet at det er nødvendig å forsikre seg om at det finnes effektive kontrollmekanismer som sørger for at etterretningstjenester ikke bruker sin makt på en ulovlig og utilbørlig måte.

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

Datatilsynet er enig med departementet i at praksis fra EMD viser etter dette at dersom innhentingen av informasjon er systematisk, informasjonen lagres over tid og utleveres til andre, vil behandlingen av opplysningene kunne anses å utgjøre et inngrep i privatlivet etter EMK artikkel 8 nr. 1, selv om informasjonen er offentlig tilgjengelig.

Ifølge høringsnotatet så vil det kunne innhentes opplysninger om «om en stor andel av befolkningen».

Etter Datatilsynets mening så blir ikke inngrepet for den enkelte og samfunnet som helhet i stor nok grad vektlagt.

Når det gjelder opplysningene som kan innhentes så vil det kunne omfatte alle typer opplysninger om en person som politisk oppfatning, medlemskap i grupper, seksuelle preferanser, helse, venner og annet nettverk, samt ytringer og meninger. Forslaget inneholder ingen begrensninger når det gjelder antall personer, nasjonalitet, kategorier data eller omfang. Det vil kunne omfatte bilder, videoer og tekst.

Innsamlingen vil også omhandle barn som skal ha særlig beskyttelse. I politidirektivet direktiv (EU) 2016/680 er dette fremhevet i fortalepunkt i fortalepunkt 50.

Innsamlingen må derfor anses som svært inngripende.

Til sammenlikning så har Det franske Datatilsynet CNIL og det engelske ICO har nylig fattet avgjørelser hvor virksomheten til Clearview AI har blitt vedtatt stanset. Clearview AI har samlet bilder, identiteter og andre opplysninger fra nettet og selger sine tjenester til bla politimyndigheter.

I vedtaket fra CNIL blir det lagt vekt på hvor inngripende denne praksisen er:

> «Indeed, it affects more than ten billion images and a significant number of people concerned. This means that there are several million people in France whose faces appear on a photograph or video publicly accessible on the Internet, and including on a social network account, that are likely to be affected by this processing. Moreover, as the database is regularly updated to integrate newly available information, the number of these people is constantly changing.
>
> In addition, this massive processing is particularly intrusive in that it collects a potentially very large amount of photographic data on a given person, to which other personal data are associated, which may reveal various aspects of their private life, such as their tastes and preferences (e.g., in terms of leisure activities) or their political or religious convictions, expressed on social networks, in blog posts or even in press articles.

> Moreover, a biometric template is created from these data, i.e., biometric data that can be considered as sensitive, which aims to identify the individual in a unique way from a photograph. Therefore, it is a facial recognition software and the company aims to enable it to be used, for instance, by law enforcement authorities to identify perpetrators and victims of offences from a photograph.»

Om masseinnhenting

EMD har også vurdert saker om masseinnhenting av informasjon, der innsamlingen som utgangspunkt ikke er systematisk eller rettet mot en konkret person. De aktuelle sakene dreier seg om hemmelig overvåkning av kommunikasjon i transitt, der både innholdet i kommunikasjonen og metadata samles inn.

EMDs nyeste avgjørelser om slik masseovervåkning er avgjørelsene i storkammersakene *Big Brother Watch and Others mot Storbritannia* og *Center för Rättvisa mot Sverige*, begge fra 25. mai 2021.

EMD la i disse sakene til grunn at masseinnsamling er en gradvis prosess, der inngrepet i individets rettigheter etter artikkel 8 tiltar underveis i prosessen, se Big Brother Watch and Others mot Storbritannia avsnitt 325 til 331. Selv på det første stadiet, der innhentingen og lagringen ikke er rettet mot konkrete individer, vil inngrepet omfattes av artikkel 8.

Domstolen har i denne sammenheng vist til at også lagring av informasjon innebærer et inngrep i rettighetene etter EMK artikkel 8. Behovet for sikkerhetsmekanismer vil imidlertid være størst på slutten av prosessen, når innholdet i kommunikasjonen blir nærmere undersøkt, se avsnitt 330. Uansett legger domstolen opp til uavhengig kontroll på alle stadier i prosessen.

I høringsnotatet 3.4.1.2 anføres det:

> «Masseinnhenting fra åpne kilder skiller seg i stor grad fra hemmelig overvåking av kommunikasjon i transitt og andre former for hemmelig overvåking. Som følge av dette har de kravene som er oppstilt i dommene nedenfor begrenset overføringsverdi for forslaget i dette høringsnotatet.»

Dette er ikke nærmere begrunnet. Det er derfor nødvendig å se på om BBW og CFR likevel vil få anvendelse på innhenting fra åpne kilder. Det første som må vurderes er hvilken informasjon som innhentes, og om det er noen reell forskjell på inngrepet.

I såkalt bulkinnhenting som er omtalt i de nevnte dommene, så er det i hovedsak metadata som hentes inn, men innholdsdata kan også hentes inn. Domstolen legger i hovedsak vekt på hvilken informasjon som kan hentes ut fra opplysningene etter analyse:

> «BBW 342. This is equally so with related communications data. As the ISR observed in its report, greater volumes of communications data are currently available on an individual relative to content, since every piece of content is surrounded by

> multiple pieces of communications data (see paragraph 159 above). While the content might be encrypted and, in any event, may not reveal anything of note about the sender or recipient, the related communications data could reveal a great deal of personal information, such as the identities and geographic location of the sender and recipient and the equipment through which the communication was transmitted. Furthermore, any intrusion occasioned by the acquisition of related communications data will be magnified when they are obtained in bulk, since they are now capable of being analysed and interrogated so as to paint an intimate picture of a person through the mapping of social networks, location tracking, Internet browsing tracking, mapping of communication patterns, and insight into who a person interacted with (see paragraph 317 above)»

Når det gjelder opplysninger innhentet fra åpne kilder, så vil det kunne omfatte alle typer opplysninger om en person som politisk oppfatning, medlemskap i grupper, seksuelle preferanser, helse, venner og annet nettverk, samt ytringer og meninger.

En innvending her kan være at dette ligger åpent tilgjengelig på internett og at en dermed ikke kan forvente samme grad av vern som for kommunikasjonsdata. Domstolen har her lagt vekt på behovet for sikkerhetsmekanismer der hvor opplysningene blir automatisk analysert.

> «BBW 330. The Court considers that Article 8 applies at each of the above stages. While the initial interception followed by the immediate discarding of parts of the communications does not constitute a particularly significant interference, the degree of interference with individuals' Article 8 rights will increase as the bulk interception process progresses. In this regard, the Court has clearly stated that even the mere storing of data relating to the private life of an individual amounts to an interference within the meaning of Article 8 (see Leander v. Sweden, 26 March 1987, § 48, Series A no. 116), and that the need for safeguards will be all the greater where the protection of personal data undergoing automatic processing is concerned (see S. and Marper, cited above, § 103).»

I høringsnotatet er det lagt vekt på at masseinnhenting fra åpne kilder i stor grad skiller seg fra hemmelig overvåking uten at dette er nærmere grunngitt. Det kan synes som om det legges vekt på at bulkinnhenting av kommunikasjonsdata er mer å regne som «skjult» enn innhenting fra åpne kilder.

Når det gjelder bulkinnhenting, så er det allment kjent at den foregår og hva den på et generelt nivå samler inn. Det er vi i Norge blant annet kjent med gjennom høringen om tilrettelagt innhenting, den offentlige debatten og lov om etterretningstjenesten som regulerer det ventede tilrettelagt innhenting. Det som er hemmelig er hvordan opplysningene behandles, hvilke søkekriterier som legges til grunn, hvem som gjenstand for en nærmere undersøkelse. I tillegg er den enkeltes rettigheter som underretning om registrering og rett til innsyn begrenset.

Dette vil i stor grad også gjelde for PSTs innhenting fra åpne kilder og det er derfor ikke nødvendig å opprettholde et skille mellom hemmelig overvåking og innhenting fra åpne kilder i denne sammenheng.

Det kan derfor argumenteres for at prinsippene fra BBW og CFR får anvendelse.

> «BBW 350. Therefore, in order to minimise the risk of the bulk interception power being abused, the Court considers that the process must be subject to "end–to–end safeguards", meaning that, at the domestic level, an assessment should be made at each stage of the process of the necessity and proportionality of the measures being taken; that bulk interception should be subject to independent authorisation at the outset, when the object and scope of the operation are being defined; and that the operation should be subject to supervision and independent ex post facto review. In the Court's view, these are fundamental safeguards which will be the cornerstone of any Article 8 compliant bulk interception regime.»

En løsning hvor innhentingen er målrettet og underlagt en uavhengig forhåndskontroll vil også være mer i tråd med EU-retten. I La Quadrature du Net and Others (sak C-511/18) fra 6. oktober 2020 slo domstolen fast at en generell og udifferensiert innsamling og lagring av slike opplysninger ville være i strid med grunnleggende rettigheter og EUs kommunikasjonsverndirektiv. Dommen åpner imidlertid for ikke-målrettet innhenting av trafikk- og lokaliseringsdata dersom lagringen begrenses til det som er strengt nødvendig basert på en reell trussel avgrenset til angitte kategorier av data, hvilke kommunikasjonsmidler som benyttes, de berørte personer og varigheten av innsamlingen og lagringstiden.

Foreslåtte kontrollmekanismer

En vurdering av hvorvidt systemet i sin helhet kan anses som proporsjonalt og «nødvendig i et demokratisk samfunn», må inneholde en vurdering av kontrollmekanismene som nødvendige garantier mot misbruk.

Formålet med slik kontroll er å forhindre misbruk og å opprettholde tilliten befolkningen har til de hemmelige tjenestene, noe som er avgjørende for å begrense de negative konsekvensene av masseovervåkning.

Det er foreslått interne kontrollrutiner i tillegg til at EOS-utvalget er tilsynsmyndighet for PST. Departementet mener at særskilte regler om lagring av opplysningene, begrensinger i bruken og etterfølgende kontroll, sett i sammenheng med de alminnelige reglene om informasjonssikkerhet, internkontroll og sporing, vil ivareta de nødvendige kravene til sikkerhetsmekanismer.

Som en del av kontrollregimet foreslår departementet at opplysningene i sin helhet skal sperres.

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

Departementet mener de sperrede opplysningene også bør kunne brukes i de tilfellene der det er åpnet etterforsking eller i forbindelse med en forebyggende sak.

Vurdering

Når det gjelder lovskravet, så vil Datatilsynet påpeke at det er vanskelig å forstå begrepet åpen tilgjengelig og hvor omfattende innsamlingen skal være.

For å vurdere om forslag kan anses som proporsjonalt må man ha en klar forståelse av hvor stort inngrepet egentlig er.

I henhold til EMDs praksis oppstår inngrepet i personvernet allerede ved selve innhentingen, uavhengig av videre bruk eller søk i opplysninger. Det er også på dette tidspunktet at de negative konsekvensene, som for eksempel nedkjølingseffekten, oppstår.

Vi mener forslaget utgjør et betydelig større inngrep i norske borgeres privatliv enn det departementet gir utrykk for, og at skadepotensialet for vårt demokratiske samfunn utvilsomt er tilstede.

I tillegg blir de negative konsekvensene for personvernet forsterket av en uklar beskrivelse av omfanget av overvåkingen. Ut fra den tekniske beskrivelsen vil systemet i praksis sannsynligvis ramme nesten hele Norges befolkning.

På grunn av vagt begrepsbruk i lovforslaget, samt uklarheter om hvem som omfattes er det stor usikkerhet rundt hvem som faktisk rammes. Dette gjør at Datatilsynet mener at kravet til klarhet og forutberegnelighet neppe er oppfylt.

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

EOS-utvalgets vil føre etterfølgende kontroll med hvem som har tilgang til de sperrede opplysningene kontroll med søk i opplysningene, og at disse kun skjer for de formål loven åpner for.

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

Forslaget innebærer også unntak fra rettsikkerhetsgarantier som underretning og innsyn. Unntaket fra retten til innsyn begrunnes i at en eventuell innsynsordning for opplysninger i PST ikke ville medføre en reell innsynsrett, idet unntakene fra innsyn på grunn av hensynet til blant annet rikets sikkerhet, kildevern og metodebruk ville komme til anvendelse i nærmest samtlige tilfeller.

Det argumenteres også for at «merverdien av innsyn være begrenset, all den tid den enkelte fritt kan søke opp informasjon som er publisert på internett om en selv.» Det vil ikke være riktig her fordi PST vil være de eneste som sitter med en oversikt som går 15 år tilbake i tid. Internett er dynamisk og opplysningene som finnes der vil forandre seg over tid. Det er for eksempel ikke lenger mulig å se hva som ble postet på Nettby – Norges største internettsamfunn med 980 000 brukere som eksisterte mellom 2006 og 2010, noe som er et eksempel på hvordan PST i fremtiden vil kunne sitte på opplysninger som ikke lenger er tilgjengelig for brukerne, noe som ytterligere forsterker maktubalansen.

Datatilsynet vurdere at dette tilsammen ikke i tråd med EMDs praksis som krever en ende til ende kontroll, hvor blant annet en uavhengig forhåndskontroll også for innhentingen og søkene vil være en sentral rettsikkerhetsmekanisme. Det mangler også en målrettethet og begrensning av innsamlingen. Datatilsynet mener helt klart at prinsippene i *Big Brother Watch and Others mot Storbritannia og Center för Rättvisa mot Sverige,* samt praksis fra Eu-domstolen blant annet *La Quadrature du Net and Others (sak C-511/18)* må legges til grunn.

Tydeliggjøring av PSTs rolle i innlands etterretning

I høringsnotatet søkes det å klargjøre PSTs rolle som innlands etterretningstjeneste, og det bes om at høringsinstansene gir sitt syn på dette.

PST har i dag ikke tilsvarende muligheter som E-tjenesten til å bidra med rettidig og relevant innenlandsetterretning. Ved at PSTs oppdrag etter politiloven i hovedsak er beskrevet som forebygging og etterforsking av konkret angitte straffbare handlinger, er tjenestens mulighet til behandle informasjon for å bidra med generelle etterretningsvurderinger og analyser knyttet til trender og utvikling i trusselbildet, begrenset. Departementet foreslår at det gis en klar hjemmel for PSTs etterretningsoppdrag i politiloven, og at det i tillegg gis en hjemmel i politiregisterloven for behandling av opplysninger for dette formålet.

Datatilsynet mener at dette endrer PSTs rolle i en slik grad at det vil få konkrete konsekvenser for personvernet, samt at det bidrar til å gjøre rollefordelingen mellom de ulike etterretnings- og polititjenestene mer uklart noe som gjør kontroll vanskeligere og kan skape en usikkerhet knyttet til i hvor stort omfang norske borgere blir utsatt for overvåking, noe som i seg selv kan bidra til nedkjølingseffekten.

I den tidligere Lov om Etterretningstjenesten (1998) uttrykte klart det såkalte territorialforbudet i § 4:

> «Etterretningstjenesten skal ikke på norsk territorium overvåke eller på annen fordekt måte innhente informasjon om norske fysiske eller juridiske personer.»

Dette uttrykte at arbeidsdelingen mellom Etterretningstjenesten og PST bør være klar og er til dels begrunnet i rettsikkerhetshensyn ved at PSTs metodebruk er underlagt domstolskontroll for å forhindre ulovlig overvåking av norske borgere i Norge.

I forslag til ny etterretningslov var ikke dette skillet like tydelig formulert, og sentrale høringsinstanser som EOS-utvalget, Riksadvokaten og PST uttalte seg om dette spørsmålet.

Riksadvokaten uttalte om unntak fra territorialforbudet blant annet:

> «Dette vil i praksis kunne åpne for innhenting av informasjon om personer og virksomheter i langt større omfang enn hva en er kjent med foregår i dag. Slik informasjonsinnhenting vil, til forskjell fra hva som er tilfellet for politiets sikkerhetstjeneste, ikke være undergitt domstolskontroll.»

PST uttalte om unntaket fra territorialforbudet:

> «I lys av den lave terskelen for iverksettelse av metodebruk for Etterretningstjenesten jf. utkastet §§ 5-1 og 5-2, og det som er skrevet over om unntakene fra territorialforbudet og de potensielle implikasjonene dette kan få for personer og virksomheter i Norge, er PST av den oppfatning at den delen av Etterretningstjenestens metodebruk som berører personer eller virksomheter innenfor norsk jurisdiksjon, bør underlegges domstolskontroll.»

Datatilsynet mener at departementet bør opprettholde skillet mellom innlands- og utenlandsetteretning og i likhet med Riksadvokaten og PST legge til grunn at metodebruk som berører personer eller virksomheter innenfor norsk jurisdiksjon, bør underlegges domstolskontroll.

Datatilsynet støtter at PSTs rolle som innlands etterretningstjeneste klargjøres, men en slik utvidelse av innlands etterretning kan ikke utvides uten at den underlegges tilsvarende kontroll som dagens metoder.

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

Forslaget innebærer at gjøres unntaket fra helt sentrale personvernprinsipper som formålsbestemthet, nødvendighet og krav til opplysningenes kvalitet.

I høringsnotatet beskrives formålene som svært vide ved at opplysningene kan brukes til etterretningsformål, samt PSTs ordinære virksomhet som er forebygging og etterforskning.

Nødvendighetsvurderingen begrunnes i stor grad av valg av metode. Det anføres at det er nødvendig at PST kan laste ned store mengder opplysninger fra internett selv om den enkelte opplysning i materialet isolert sett ikke vil være nødvendige for formålet, uten å drøfte om en mer målrettet metode kunne ha oppfylt formålene.

Det er grunn til å påpeke at målretting står helt sentralt både i praksis fra EMD og EU-domstolen.

Det foreslås også unntak fra politiregisterloven § 6 om at kravene til at opplysningene som behandles skal være relevante og korrekte.

Når informasjon publiseres på internett vil PST ikke ha noen mulighet til å vurdere om den enkelte opplysning faktisk er korrekt. Opplysningene vil kunne anses korrekte i den forstand at de fremkommer på den måten de har blitt publisert, uavhengig av om de reelt sett stemmer.

Datatilsynet vil understreke betydningen av korrekte opplysninger ved bruk av automatiserte analyseverktøy og eventuell bruk av kunstig intelligens, og den fare for algoritmeskjevhet (bias) det kan medføre.

Det foreslås også et unntak fra § 7, som gir anvisning på at behandling av særlige kategorier av opplysninger bare kan finne sted dersom det er strengt nødvendig ut fra formålet med behandlingen.

Unntaket begrunnes i at:

> «Mange publiserer denne typen opplysninger på internett, eksempelvis om politisk eller religiøs overbevisning, seksuell orientering osv.»

Det er i utgangspunktet helt riktig, men det er under forutsetning av at myndighetene ikke registrerer og analyserer disse opplysningene. Det er ikke lenger siden enn 2014 hvor EOS-utvalget problematiserte behandling av opplysning om politisk overbevisning i sin særskilte melding i 2014, mens det nå åpnes for å samle inn denne type opplysninger om «om en stor andel av befolkningen». Det må også tas med i betraktningen at denne type informasjon om andre mot deres vilje og på en ulovlig måte.

Problemet er at selv om opplysningene lagres ustrukturert, så kan analyseverktøy raskt og enkelt kategorisere opplysningene, noe en må tro at hensikten med systemet også er.

Sletting

Det er foreslått en slettefrist på 15 år noe som innebærer at opplysninger som enten blir korrigert, slettet eller oppdatert på internett forblir lagret hos myndighetene.

En betydelig del av disse opplysningene vil være ytringer eller handlinger gjort av barn.

Datatilsynet kan ikke se noen tungtveiende begrunnelse for en så lang lagring. Når det gjelder henvisningen til etterretningstjenesteloven § 9-8 om sletting av rådata i bulk, så omfatter i følge høringsnotatet pkt. 8.6.2. «rådata i bulk» lite informasjon om norske borgere, noe som heller ikke er formålet med innsamlingen.

> «Departementet viser til at innhenting av rådata i bulk ikke har til hensikt å samle inn informasjon om personer og virksomheter i Norge. Dette er snarere informasjon som teknisk uunngåelig og uintendert «følger med på lasset», og som for de fleste former for bulkinnsamling utgjør en svært liten andel av den samlede datamengden.»

Hvis en skal velge en bestemmelse fra etterretningsloven som inspirasjon så er nok § 7-7 om innhenting og lagring av metadata i bulk etter tilrettelagt innhenting mer relevant, med en lagringstid på 18 måneder.

Konklusjon

I NOU 2012: 14 Rapport fra 22. juli-kommisjonen punkt 16.6 om åpne kilder og overvåking av internett står det:

> «Vi er ikke overbevist om at verdien av å overvåke generell trafikk på nettet ved bruk av søkeord oppveier den demokratiske omkostningen ved slik overvåking av den alminnelige meningsutveksling.»

Datatilsynet deler dette synspunktet og mener at systemet ikke bør innføres. Hvis systemet likevel innføres, så bør det i mye sterkere grad ivareta rettsikkerhetsgarantier med utgangspunkt i praksis fra EU-domstolen og EMD.

Med vennlig hilsen

Bjørn Erik Thon
direktør

Jan Henrik Mjønes Nielsen
juridisk seniorrådgiver

Dokumentet er elektronisk godkjent og har derfor ingen håndskrevne signaturer