Norges nasjonale institusjon for menneskerettigheter

Justis- og beredskapsdepartementet
Postboks 8005 Dep
0030 Oslo

Deres referanse: [Deres ref.]
Vår referanse: 2018/196
Dato: 31/08/2018

Innspill til mandat til personvernkommisjon

1. Innledning

Vi viser til høringsbrev av 11. juli 2018 fra Justis- og beredskapsdepartementet vedrørende utformingen av mandatet til en *personvernkommisjon,* med høringsfrist 31. august 2018.

Norges nasjonale institusjon for menneskerettigheter («NIM») har som hovedoppgave å fremme og beskytte menneskerettighetene i tråd med Grunnloven, menneskerettsloven og den øvrige lovgivningen, internasjonale traktater og folkeretten for øvrig.[1] NIM skal blant annet gi råd til Stortinget, regjeringen og andre offentlige organer om gjennomføringen av menneskerettighetene.[2]

NIM mener det er positivt at Regjeringen skal sette ned en personvernkommisjon som skal vurdere personvernets stilling i Norge. Det er snart ti år siden den forrige personvernkommisjonen la frem sin rapport, og siden den gang har det skjedd betydelige endringer både på det teknologiske og det rettslige området.[3] Statens myndigheter skal respektere og sikre retten til privatliv.[4] En helhetlig vurdering og kartlegging av personvernets stilling bidrar til å styrke statens forutsetninger for å ivareta dette ansvaret.

I følgende punkt 2 vil vi gi noen overordnede innspill til kommisjonens mandat. Deretter vil vi i punkt 3 gå nærmere inn på konkrete problemstillinger vi mener kommisjonen bør ta opp i sin utredning.

2. Behovet for en bred og helhetlig analyse av personvernets stilling

Begrepet «personvern» blir gjerne forstått slik at det «dreier seg om ivaretakelse av personlig integritet; ivaretakelse av enkeltindividers mulighet for privatliv, selvbestemmelse (autonomi) og selvutfoldelse.»[5] Det er med andre ord snakk om et sammensatt og temmelig omfattende fenomen. Derfor er det etter NIMs syn behov for

1 NIM-loven § 1 annet ledd.

2 NIM-loven § 3 første ledd, bokstav b; Innst. 216 L (2014–2015) s. 3

3 NOU 2009: 1 Individ og integritet – personvern i det digitale samfunnet. Utredningen ble fulgt opp i Meld. St. 11 (2012–2013) Personvern – utsikter og utfordringar.

4 Jf Grunnloven § 92 og 102 og EMK artikkel 8 jf. 1.

5 NOU 2009: 1, punkt 4.1.5. Lønning-utvalget la samme forståelse til grunn i sin rapport, se Dokument 16 (2011–2012) s. 173.

en bred analyse, der man utreder både verdimessige, faktiske og rettslige sider ved personvernets stilling i dagens samfunn. NIM mener en slik helhetlig tilnærming er viktig, men vil samtidig understreke viktigheten av at kommisjonen ikke blander sammen de ulike aspektene i sine analyser.

Den *verdimessige* analysen av personvernet bør særlig ta sikte på å drøfte hvilken funksjon personvernet har og bør ha i vårt samfunn. I tillegg til å vurdere hvilke underliggende verdier reglene om personvern skal ivareta, bør kommisjonen utrede hvilke andre verdier og hensyn personvernet kan komme i konflikt med og hvilke prinsipper som bør gjelde for avveiningen mellom disse.

I en analyse av personvernets *faktiske* sider, er det først og fremst naturlig å vurdere hvordan den teknologiske utviklingen har påvirket og kommer til å påvirke personvernets stilling. Men også andre faktiske forhold bør etter NIMs syn tas i betraktning, som for eksempel kriminalitetsbildet, geopolitiske forhold, multinasjonale selskapers rolle i samfunnet og hvordan kommunikasjonsmønstrene våre har endret seg. Kommisjonen bør særlig ta sikte på å fremheve utviklingstrekk som kan sette personvernet under press.

Den *rettslige* analysen bør bestå i en grundig kartlegging av innholdet i statens konstitusjonelle og internasjonale forpliktelser på området, og en vurdering av i hvilken grad gjeldende lovverk og praksis er i samsvar med disse forpliktelsene. Her vil det særlig være viktig å foreta en gjennomgang og analyse av nyere rettspraksis fra Høyesterett, Den europeiske menneskerettsdomstolen (EMD) og EU-domstolen. Det bør slik NIM ser det være en del av kommisjonens mandat å foreslå lovendringer dersom den finner at deler av lovverket strider mot statens menneskerettslige forpliktelser.

3. Problemstillinger NIM mener kommisjonen bør ta opp

3.1. Innledning

I de følgende avsnittene vil vi presentere enkelte problemstillinger vi mener det er naturlig at den nye personvernkommisjonen tar opp i sin utredning. Listen er verken uttømmende eller i prioritert rekkefølge. Selv om det på noen av områdene er pågående lovgivningsprosesser, mener NIM at kommisjonen uansett bør ta stilling til spørsmålene. Blant annet vil det komme rettspraksis fra EMD som kan aktualisere nye vurderinger av ulike regelverk.[6] Måten kommisjonen utreder problemstillingene på vil allikevel kunne avhenge av hvordan de ulike lovgivningsprosessene forløper.

3.2. En samlet gjennomgang av politiets og PSTs hjemler for bruk av skjulte tvangsmidler

[6] EMD skal blant annet behandle saker mot Østerrike, Storbritannia og Frankrike som handler om landenes overvåknings- og etterretningstjenester, se faktaarket «Mass surveillance», tilgjengelig på domstolens hjemmesider.

Politiet og PST har gjennom flere lovendringer de siste 20 årene fått en betydelig utvidet adgang til å bruke skjulte tvangsmidler i etterforsknings-, avvergings- og forebyggingsøyemed.[7] Reglene ble sist evaluert på en helhetlig måte av Metodekontrollutvalget i 2009.[8]

NIM mener det nå er behov for en samlet gjennomgang av politiets og PSTs hjemler for bruk av skjulte tvangsmidler, særlig i lys av at lovendringene har vært fragmentariske og kommet i flere etapper. I den sammenheng bør kommisjonen blant annet foreta en evaluering av endringene i straffeprosessloven § 222d og politiloven § 17d som ble vedtatt i 2016. Bestemmelsene gir politiet og PST adgang til å ta i bruk skjulte tvangsmidler for å forebygge og avverge kriminalitet. NIM konkluderte i en temarapport med at enkelte sider ved lovendringene trolig strider mot husransakelsesforbudet i Grunnloven § 102 første ledd andre punktum.[9] I årsmeldingene for 2016 og 2017 anbefalte vi Regjeringen å utrede i hvilken utstrekning tvangsmiddelbruk i medhold av bestemmelsene er forenlig med Grunnlovens husransakelsesforbud.[10]

Vi nevner for øvrig at Menneskerettskomiteen uttrykte bekymring for lovendringene av 2016 i sin nylige vurdering av Norges statspartsrapport under FN-konvensjonen om sivile og politiske rettigheter.[11]

Vi minner også om Justis- og beredskapsdepartementet brev til Stortingets justiskomite, datert 25. juni 2018, om oppfølgingen av NIMs årsmelding for 2016. Ad anbefaling nr. 4 på s. 3–4 vises det til regjeringsplattformen hvor det fremgår at regjeringen skal oppnevne et offentlig utvalg som blant annet skal evaluere metodebruken som har grunnlag i de forannevnte lovendringene, samt forholdet til Grunnloven. Det fremstår naturlig at dette tilkommer personvernkommisjonen.

3.3. Behandlingen av informasjon innhentet ved kommunikasjonskontroll mv.

En annen viktig side av myndighetenes overvåkningsvirksomhet er hvordan den innsamlede informasjonen blir behandlet. Både lagring og videre bruk av slikt materiale utgjør selvstendige inngrep i privatlivet, og må dermed ha hjemmel i lov, ivareta et legitimt formål og være forholdsmessig.[12] Lovhjemler for lagring og videre bruk må oppfylle visse kvalitative krav til tilgjengelighet og presisjon.[13]

---

[7] For en gjennomgang av sentrale utviklingstrekk, se Jon Wessel Aas, «Pressefrihetens kår i 2014: Ett skritt frem – og to tilbake?», *Status for ytringsfriheten i Norge – Fritt Ords monitorprosjekt*, 2014, punkt 4. I tillegg kommer lovendringene i 2016, se straks nedenfor i brødteksten.

[8] NOU 2009: 15.

[9] Se «Grunnloven § 102: Hva må ikke finne sted, unntatt i hvilke tilfeller?», tilgjengelig på våre hjemmesider.

[10] Se årsmeldingen for 2016 s. 119 og årsmeldingen for 2017 s. 33. Årsmeldingene ligger tilgjengelige på våre hjemmesider.

[11] CCPR/C/NOR/CO/7 avsnitt 20.

[12] Se for eksempel Rt. 2014 s. 1105 (avsnitt 29–30), med videre henvisning til praksis fra EMD.

[13] Rt. 2014 s. 1105 avsnitt 30.

Det har flere ganger de siste årene blitt påpekt at politiets praksis for sletting av materiale fra kommunikasjonskontroll neppe er i tråd med gjeldende regelverk. Dette ble senest tatt opp av Kontrollutvalget for kommunikasjonskontroll i en særskilt melding i juni 2018.[14] NIM påpekte tilsvarende menneskerettslige utfordringer ved utformingen og anvendelsen av dette regelverket i brev til Justis og beredskapsdepartementet den 2. juli 2018. Straffeprosessloven § 216 g om sletting av materiale ble endret av Stortinget i 2013, men lovendringen har ennå ikke trådt i kraft. Høsten 2017 ble for øvrig ytterligere endringsforslag sendt på høring.

Videre reiser selve bruken av overskuddsmateriale flere problemstillinger, blant annet knyttet til bruk for å avverge og etterforske annen kriminalitet enn den saken som aktualiserte innhentingen. Enkelte av disse spørsmålene er tatt opp i vår høringsuttalelse til Justisdepartementets høringsnotat om behandling av overskuddsinformasjon fra kommunikasjonskontroll mv.[15]

NIM mener at kommisjonen bør foreta en gjennomgang av regelverket for behandling av informasjon innhentet ved kommunikasjonskontroll mv., og vurdere det opp mot gjeldende menneskerettslige forpliktelser.

3.4. Deling av hemmelig innhentet informasjon mellom politiet, PST og E-tjenesten

Også deling av hemmelig innsamlet informasjon utgjør et selvstendig inngrep i retten til privatliv. Dermed må det foreligge et hjemmelsgrunnlag for deling, og delingen må ivareta legitime formål og skje på en forholdsmessig måte. En praktisk viktig form for deling er informasjonsutveksling mellom de ulike overvåkningstjenestene. Ettersom innhentingskapasiteten og volumet har økt, og må antas å øke, er det naturlig at mer informasjon også blir delt mellom tjenestene. I tillegg til at det er et behov for klare og presise hjemmelsgrunnlag, må det være mekanismer som ivaretar at deling kun skjer når det er forholdsmessig, samt at oppbevaringen og bruken hos den informasjonen tildeles er i tråd med menneskerettslige krav.

NIM mener derfor at kommisjonen også bør gjennomgå regelverket for deling av hemmelig informasjon mellom de ulike tjenestene.[16]

3.5. Kontroll med hemmelig overvåkning

Et grunnleggende rettsstatlig og menneskerettslig krav er at det finnes kontrollmekanismer som kan påse at overvåkningsmyndighetene opptrer i tråd med

[14] «Særskilt innberetning etter kommunikasjonskontrollforskriften § 17 – sletting av materiale fra kommunikasjonskontroll m.m.». At politiets praksis ikke fulgte slettingsbestemmelsene ble påpekt så langt tilbake som i 2009, se Metodekontrollutvalgets rapport i NOU 2009: 15, punkt 24.1.

[15] Høringsuttalelsen ligger tilgjengelig på våre hjemmesider.

[16] Enkelte sider av dette ble tatt opp i høringsuttalelsen som er nevnt i forrige fotnote.

regelverket. I nyere saker om hemmelig overvåkning som har kommet opp for EMD har domstolen lagt stadig større vekt på hvilke kontrollmekanismer som er tilgjengelige i nasjonal rett. Kontrollmekanismenes innretning har i flere avgjørelser vært av stor betydning for forholdsmessighetsvurderingen etter EMK artikkel 8.[17] I følge EMD bør kontrollfunksjoner ideelt sett utøves av en uavhengig domstol, men også andre typer organer kan stå for kontrollvirksomheten, forutsatt at de er uavhengige og har tilstrekkelig myndighet til å utøve en *effektiv og løpende kontroll*.[18]

Vi nevner også at Menneskerettskomiteen nylig har bedt norske myndigheter om å «ensure the effectiveness and independence of a monitoring system for surveillance activities».[19]

NIM mener i lys av dette at kommisjonen bør foreta en evaluering av det nåværende systemet for kontroll med ulike former for hemmelig overvåkning. Evalueringen bør særlig omfatte systemet for alminnelig domstolskontroll med bruk av straffeprosessuelle tvangsmidler og Kontrollutvalget for kommunikasjonskontroll og EOS-utvalget sin virksomhet. Videre bør kommisjonen se nærmere på kontrollmekanismene for det foreslåtte «Digitalt grenseforsvar», som omtales nærmere nedenfor.[20]

Et særskilt aspekt NIM mener kommisjonen bør undersøke er om nåværende systemer sikrer at domstoler og kontrollorganer har tilstrekkelig kunnskap og kompetanse til å føre en effektiv kontroll. Både de juridiske og de teknologiske spørsmålene som reises i overvåkningssaker kan være svært komplekse, og særlig skjæringspunktet – når rettsreglene skal anvendes i konkrete tilfeller – fordrer god forståelse om begge fagområder.

3.6. Etterretningstjenestens overvåkningspraksis og lovgrunnlaget for praksisen

En problemstilling som har fått en del oppmerksomhet de senere årene er Etterretningstjenestens overvåkningspraksis. Diskusjonen har handlet om hvorvidt tjenesten har tilstrekkelig lovhjemmel for å gjøre søk i metadata knyttet til norske borgere i Norge. EOS-utvalget la frem en særskilt melding til Stortinget om spørsmålet i 2016, og vi omtalte saken i vår årsmelding for 2016. I 2018 fikk saken oppmerksomhet i mediene.[21] Regjeringen har varslet at det skal sendes forslag til lovendring på høring høsten 2018.

---

[17] Se blant annet *Centrum för Rättvisa v. Sverige*, *Szabó og Vissy v. Ungarn*, sak 37138/14, *Roman Zakharov v. Russland*, sak 47143/06 og *Klass m.fl. v. Tyskland,* sak 5029/71.

[18] Se blant annet *Centrum för Rättvisa v. Sverige* avsnitt 153.

[19] CCPR/C/NOR/CO/7 avsnitt 21.

[20] I Lysne II-utvalgets konseptbeskrivelse ble det foreslått en «DGF-domstol», se rapporten «Digitalt grenseforsvar», avgitt 26. august 2016, punkt 9.3. NIM ga i sin høringsuttalelse uttrykk for at kontrollen burde ligge til de alminnelige domstoler. Høringsuttalelse ligger tilgjengelig våre hjemmesider.

[21] Se https://www.nrk.no/norge/stortinget-krever-svar-fra-forsvarsministeren-om-overvakningsbase-1.13949261.

NIM mener kommisjonen bør få i mandat å vurdere Etterretningstjenestens overvåkningspraksis, og eventuelt evaluere bebudede lovendringer dersom disse kommer på plass.

3.7. Digitalt grenseforsvar

En annen sak som har fått mye oppmerksomhet er forslaget om et nytt overvåkningsprogram for E-tjenesten, kalt Digitalt grenseforsvar (DGF). Konseptet ble lagt frem av Lysne II-utvalget i 2016.[22] Forslaget går kort fortalt ut på masseinnsamling av kommunikasjon som knytter landegrensene, der innsamling av metadata om kommunikasjonen er den mest sentrale delen. Forslaget slik det ble lagt frem vil innebære at store deler av kommunikasjonen nordmenn foretar seg vil bli samlet inn av E-tjenesten.

Lysne II-utvalgets rapport inneholdt bare en konseptuell beskrivelse av et digitalt grenseforsvar, mens en lovproposisjon er varslet løpet av høsten 2018. NIM mener kommisjonen bør vurdere både hvilke implikasjoner et slikt forslag vil ha for personvernets stilling i samfunnet som helhet, og i hvilken grad forslaget er i tråd med menneskerettighetene.

3.8. Rettslig regulering av ansiktsgjenkjenningsteknologi

Ansiktsgjenkjenningsteknologien har utviklet seg betydelig de senere årene. Teknologien gir uante muligheter for offentlige og private aktører, både på godt og vondt. Slike virkemidler kan potensielt ha svært negative konsekvenser for personvernet, og behovet for rettslig regulering vil melde seg med tiltakende styrke. Dette er erkjent av blant annet Microsoft, som – selv om selskapet har kommersielle interesser på området – har bedt amerikanske myndigheter komme på banen med rettslig regulering.[23]

NIM mener kommisjonen bør vurdere om det er behov for særskilt regulering av bruken av ansiktsgjenkjenningsteknologi i norsk rett.

4. Avslutning

NIM vil avslutningsvis påpeke at personvernet er et av de menneskerettsområdene som er relevant for store deler av befolkningen i det daglige. Samtidig er det et felt hvor det er vanskelig for den enkelte å orientere seg, på grunn av hyppig utvikling og til dels kompleks og uoversiktlig teknologi og rettslig regulering. NIM mener derfor at det bør inngå som en del av kommisjonens mandat å drive utadrettet virksomhet og allmennopplysning om personvernets stilling.

---

[22] Tilgjengelig på Regjeringens hjemmesider.

23 «Facial recognition technology: The need for public regulation and corporate responsibility», tilgjengelig på Microsoft sine hjemmesider.

Vennlig hilsen
for Norges nasjonale institusjon for menneskerettigheter

Adele Matheson Mestad	Kristian Reinert Haugland Nilsen
Assisterende direktør	Seniorrådgiver

Dette dokumentet er elektronisk godkjent og har dermed ingen signatur.