POLITIET
POLITIDIREKTORATET

Justis- og beredskapsdepartementet
Postboks 8005 Dep
0030 OSLO

NATIONAL POLICE DIRECTORATE

Deres referanse:	Vår referanse:	Sted, Dato
18/3955	201803252-11 008	Oslo, 03.10.2018

HØRINGSSVAR - PERSONVERNKOMMISJON - INNSPILL TIL MANDAT

1. INNLEDNING

Vi viser til Justis- og beredskapsdepartementets høringsbrev av 11. juli 2018. Frist for høringen er satt til 31. august 2018, og vi viser til senere dialog med departementet om frist.

Politidirektoratet har forelagt høringen for underliggende enheter. Vedlagt følger høringsuttalelser fra Oslo og Agder politidistrikt, Kripos og Økokrim. Sistnevnte særorgan hadde ingen merknader til høringen.

I forbindelse med at regjeringen skal nedsette en personvernkommisjon som skal vurdere personvernets stilling i Norge ber departementet om innspill til utforming av personvernkommisjonens mandat. Personvernkommisjonen skal ifølge høringsbrevet og Jeløya-plattformen se på personvern i justissektoren, og hvordan personvernet kan sikres ved økt bruk av digitale løsninger, herunder rettighetene til brukere av sosiale medier. I tillegg skal mandatet også inkludere et særlig oppdrag om å vurdere tilstanden for barns personvern, herunder komme med tiltak for å styrke dette.[1]

Politidirektoratet stiller seg positive til at det skal nedsettes en personvernkommisjon som skal se på personvernets stilling i justissektoren. Vi viser til vedlagte høringsuttalelser fra underliggende enheter, der samtlige som har gitt innspill til direktoratet stiller seg positive til etableringen av en ny personvernkommisjon, herunder en prioritering av offentlige etaters behandling av personopplysninger og informasjonsutveksling.

Etter Politidirektoratets oppfatning kan debatten om personvernets stilling i justissektoren synes å bære preg av et for begrenset syn på innholdet i begrepet personvernet. Det blir ofte en debatt som er preget av at personvernets største trussel fremstilles å være myndighetenes tilgang på personopplysninger. Og videre at politiets utvidede adgang til enkelte målrettede metoder som følge av blant annet teknologiutviklingen, først og fremst er begrunnet i politiets overvåkningstrang. Politiets metodebruk og tilgang på personopplysninger er selvsagt relevant for personvernet, men personvern er også så mye mer enn dette.

[1] se Stortingets anmodningsvedtak 588 og Representantforslag 68 S (2017–2018).

Politidirektoratet

Post: Postboks 8051 Dep., 0031 Oslo
Besøk: Fridtjof Nansens vei 14/16
Tlf: 23 36 41 00
Faks: 23 36 42 96
E-post: politidirektoratet@politiet.no
Org. nr.: 982 531 950
Giro: 7694.05.18020
www.politi.no

Personvernkommisjonen bør derfor *gis i oppdrag å gjennomføre en grundig gjennomgang og avgrensning av personvernet*. Det vil si hva det er et vern av – hvilke verdier ønsker vi å verne, og hva som er de reelle truslene mot personvernet. Dette fremstår nå som et helt nødvendig utgangspunkt for objektivt å få satt premissene for den videre debatten. Debatten er og har vært preget av sterke motsetninger, og til dels sprikende utgangspunkt og premisser. Debatten har også en tendens til å sette likhetstegn mellom *personopplysnings*vern og personvern, noe som etter vårt syn blir alt for snevert. For at politi- og påtalemyndighet skal settes i stand til å ivareta sine oppgaver er det viktig å få beskrevet et (utvidet) personvernbegrep som tydelig omfatter individenes (samfunnets) interesse i at kriminalitet forebygges, og oppklares. Politidirektoratet mener at kommisjonen i det minste tydelig bør definere hvilken forståelse av begrepet personvern de legger til grunn.

Offentlige etaters behandling av personopplysninger og informasjonsutveksling

Politiloven § 2 stadfester at politiets primæroppgave er å bekjempe kriminalitet. Dette kan omtales som kriminalitetsbekjempelsesfunksjonen, som tar opp i seg politiets oppgaver innen forebygging, etterforsking og strafforfølging. Videre må politiets oppgaveløsning skje innenfor rammen av Grunnloven, menneskerettighetsforpliktelsene og relevant annen lovgivning.

Hensyn til personvern og privatlivets fred er grunnleggende rettigheter. Samtidig er det for politiets del viktig at disse hensynene avstemmes mot hensynet til en effektiv kriminalitetsbekjempelse, herunder hensyn til fornærmede og borgernes trygghetsfølelse i samfunnet.

Når ovennevnte hensyn skal veies mot hverandre, er det særlig teknologiutviklingen som har skapt et forsterket behov for en grundig gjennomgang av personvernets kår generelt, og personvern i relasjon til kriminalitetsutviklingen og politiets arbeid og metoder spesielt. Teknologi og internett endrer kriminaliteten – både med hensyn til kompleksitet, omfang samt hvem, hvor og hvordan den rammer.

Politiet har som mål i virksomhetsstrategien at vi i 2025 skal ligge i forkant av kriminaliteten, herunder levere kvalitet i alle ledd. Vi skal ha kriminalitetsforebygging som hovedstrategi og sette andre i stand til å forebygge.

Politiet må i fremtiden være forberedt på å yte mer for mindre, finne smartere løsninger og imøtekomme endringer og reformer i langt større grad enn i dag. Presset på offentlig sektor vil øke betydelig og en god måte å møte disse kravene på, er gjennom inkludering og involvering av samarbeidspartnere og utnytte teknologi som er tilgjengelig. Vi må øke handlingsrommet gjennom innovasjon og partnerskap samt evne å benytte den teknologiske utviklingen langt raskere enn det som er tilfelle i dag. For politiets del vil det være avgjørende for vår evne til å løse vårt samfunnsoppdrag - forebygge og bekjempe kriminalitet.

Videre mener Politidirektoratet at personvernkommisjonen må *gis i oppdrag å gjennomgå de regulatoriske tiltak som har påvirket personvernets kår de siste 20 år*. Dette gjelder både de tiltak som kan oppfattes å utfordre personvernet (f.eks politiets metoder) og de som bidrar til å styrke personvernet (f.eks sletteplikt, personopplysningslov, GDPR). I debatten ser vi en tendens til at utviklingen blir fremstilt til ensidig å ha svekket personvernet. Politidirektoratet mener den videre debatten fortjener en objektiv og grundig gjennomgang av hvorvidt dette faktisk er tilfellet. En slik gjennomgang og oversikt vurderes derfor som nødvendig. Dersom departementet finner at et slikt oppdrag blir for omfattende, kan det vurderes å begrense

oppdraget til å gi en oversikt over sentrale regulatoriske tiltak og en drøftelse av status for personvern/effekter av tiltakene på denne bakgrunn.

Trekkene ved samfunnsutviklingen understøtter behovet for at politiet har klare hjemler for adgang til å bruke og utlevere informasjon uten at personvernet setter for store begrensinger i delingsadgangen. I tråd med den teknologiske utviklingen og mulighetene denne gir er det viktig at politiet samtidig har et balansert forhold til ulike hensyn som gjør seg gjeldende, ved å avveie hensynene til en effektiv kriminalitetsbekjempelse og hensynet til personvernet. Med utgangspunkt i ovennevnte er det dessuten nødvendig å presisere at det *ikke* er slik at effektiv kriminalitetsbekjempelse i sin natur er en trussel mot personvernet. Politiets evne til kriminalitetsbekjempelse vil på gitte områder også være helt nødvendig for å bevare og styrke personvernet og den reelle retten til privatliv.

Direktoratet mener at utformingen av mandatet til kommisjonen bør ses i sammenheng med endringer i samfunns- og kriminalitetsbildet. Videre er Politidirektoratet av den oppfatning at mandatet til kommisjonen ikke bør favne for bredt. Kripos fremholder samme synspunkt.

Grensedragning mellom ulike lover

Politidirektoratet mener at kommisjonen bør se på grensedragningen mellom personopplysningsloven, forvaltningsloven og arkivloven. I praksis ser vi at regelverk knyttet til personvern, forvaltningsrettslige regler om taushetsplikt og utlevering og regelverk knyttet til arkiv/lagring ofte krysses og reiser flere problemstillinger. Politidirektoratet vil i høringssvaret berøre aktuelle temaer som omhandler taushetsplikt og utlevering, da disse reglene også er motivert ut fra personvernhensyn. Vi viser i den forbindelse til høringen om endringer i politiregisterloven, arkivloven og straffeprosessloven – sletting i politiets registre mv.[2]

Politidirektoratet er også kjent med at forvaltningslovutvalget i brev fra Justis- og beredskapsdepartementet 19. januar 2017 har fått en tilleggsbestilling om å vurdere forvaltningslovens regler om taushetsplikt opp mot etatenes behov for informasjon fra andre myndigheter for å bekjempe kriminalitet. Forvaltningslovutvalget er i tilleggsbestillingen bedt om å se hen til en rapport[3] fra 2015 som kartla utfordringer med dagens regelverk, der det er vist til alternative måter å regulere dette på, herunder svenske regler ("generalklausul" og særlige bestemmelser om organisert kriminalitet). Følgende fremgår av departementets tilleggsbestilling:

> *Dagens regelverk rundt taushetsplikt og informasjonsdeling kan være til hinder for en effektiv kriminalitetsbekjempelse. Forvaltningslovutvalget skal for å imøtekomme det offentliges behov for bedre adgang til informasjonsdeling utrede forvaltningslovens regler om taushetsplikt. Det skal utarbeides regelverk som muliggjør utveksling mellom offentlige kontrollorgan og politi etter interesseavveininger mellom hensynet til utlevering og hensynet til taushetsplikten.*

Sammensetning av kommisjonen

Politidirektoratet støtter Kripos og Oslo politidistrikt uttalelse, som begge fremholder behovet for at kommisjonen har en bred sammensetning med blant annet teknologer, samfunnsvitere

[2] Justis- og beredskapsdepartementets referanse 16/7853.
[3] Rapport avgitt 1. desember 2015 «*Rapport om styrket informasjonsdeling mellom kontrolletatene, politi og private for bekjempelse av kriminalitet. Kartlegging av svakheter ved regelverket og forslag til eventuelle lovendringer*»

og jurister. Politidirektoratet er også enig i at kommisjonen bør være sammensatt av representanter fra justissektoren, herunder med kunnskap og kompetanse om hvordan politiet behandler og bruker opplysninger, og politiets registre og andre systemer, samt personer med politifaglig bakgrunn. Politiet kan bidra i utvelgelsen av eventuelle personer som kan ivareta slike perspektiver.

Offentlige etaters bruk av opplysninger og bruk til andre formål

Kripos fremholder at "det kan (…) vurderes om en undersøkelse av offentlige etaters bruk av personopplysninger til andre formål enn det de ble innhentet for bør være en del av kommisjonens mandat" og viser i den forbindelse til Finansdepartementets høringsnotat av 24. mai 2018 om adgang for Skatteetaten og Tolletaten til å bruke personopplysninger ved utvikling og testing av IT-systemer.[4]

Politidirektoratets støtter merknaden til Kripos, og viser i den forbindelse til direktoratets høringssvar 10. august 2018. Direktoratet imøteså at formålet med departementets forslag til endringer nettopp var for å klargjøre *at* skatteeten og Tolletaten har rettslig adgang til å bruke personopplysninger til det angitte formålet, nemlig utvikling og testing av IT-systemer.[5]

Vi viser også til Justis- og beredskapsdepartementets brev av 9. mai 2018 med høring om forslag til ny bestemmelse i personopplysningsloven om adgang til utveksling av personopplysninger for å bekjempe arbeidslivskriminalitet, samt Politidirektoratets høringsuttalelse av 30. mai 2018.[6] Direktoratet støttet her forslag om en generell hjemmel i personopplysningen (forsag til ny § 12) som et *supplerende* rettsgrunnlag for utlevering/utveksling av informasjon mellom offentlige organer, herunder hjemmel for viderebehandling til nye formål. I høringssvaret påpekte vi samtidig at den nye hjemmelen i praksis vil ha begrenset nedslagsfelt all den tid den ikke vil ha innvirkning på utveksling av taushetsbelagt informasjon.

Politidirektoratet mener kommisjonen bør klarlegge taushetspliktreglene for offentlige organer, herunder personvernet opp mot det offentliges rett/plikt til å dele opplysninger for å bidra til oppfyllelse av andre etaters oppgaver mv. etter eget regelverk. De hensyn som taler for og mot en slik informasjonsutveksling bør også klarlegges.

Offentlige etaters gjenbruk av informasjon

Både Agder politidistrikt og Kripos mener at politiet har behov for å kunne gjenbruke opplysninger. Kripos peker i den forbindelse blant annet på et prinsipp som løftes frem i stortingsmeldingen *Digital agenda for Norge*[7] om at "[f]orvaltningen skal gjenbruke informasjon i stedet for å spørre brukerne på nytt om forhold de allerede har opplyst"[8]. Politidirektoratet støtter Agder politidistrikts og Kripos' merknader, og er enig i at gjenbruk av opplysninger innebærer et mindre inngrep i personvernet generelt sett.

Politiet inngår i tverrfaglig samarbeid

I forlengelsen av gjenbruksproblematikken bemerker Kripos at økt samhandling mellom offentlige etater, med ulike regelsett som regulerer behandlingen av personopplysninger, kan medføre et juridisk landskap som det er vanskelig å navigere i. Kripos viser til akrim-satsningen som illustrasjon for aktuelle problemstillinger som oppstår, og skriver følgende:

[4] Departementets saksnummer 18/1077.
[5] Politidirektoratets saksreferanse 201802706 og Finansdepartementets referanse 18/1077.
[6] Justis- og beredskapsdepartementets referanse 18/2673 og Politidirektoratets høringssvar 30.05.2018 med referanse 201802191.
[7] Beskriver regjeringens hovedmål og prioriteringer i IT-politikken.
[8] St. 27 (2015–2016) del 2 punkt 7.

> Som eksempel kan akrim-satsingen eller etablering av tjenesten Nød-SMS trekkes frem. Når flere offentlige organer inngår et samarbeid, oppstår det mange og til dels vanskelige problemstillinger; hvem blir behandlingsansvarlig for opplysningene, hvilket regelsett må legges til grunn, hvordan skal opplysninger utveksles, når det sammenstilles opplysninger fra flere ulike enheter som blir et nytt kunnskapsgrunnlag - hva kan disse opplysningene brukes til, hjemmel til å utlevere, men ikke behandlingsgrunnlag for å behandle mottatte opplysninger, samt risiko knyttet til etablering av delt behandlingsansvar, for å nevne noen.

Oslo politidistrikt fremhever betydningen av samhandling med kontrollmyndigheter, og peker i sin uttalelse på side 4 at kommisjonen bør drøfte rammene for lovlig utveksling av personopplysninger mellom politiet og offentlige kontrollmyndigheter.

Politidirektoratet deler Kripos og Oslo politidistrikts merknader og beskrivelse av aktuelle problemstillinger som oppstår ved tverrfaglig samarbeid. Politidirektoratet viser også i denne forbindelse ovennevnte høring om forslag til ny bestemmelse i personopplysningsloven om adgang til utveksling av personopplysninger for å bekjempe arbeidslivskriminalitet, samt Politidirektoratets høringsuttalelse av 30. mai 2018.[9] Direktoratet støttet her forslag om en generell hjemmel i personopplysningen (forsag til ny § 12) som et supplerende rettsgrunnlag for utlevering/utveksling av informasjon mellom offentlige organer. Særlig fremheves at direktoratet i sitt høringssvar pekte på behovet for tydelige hjemler for utlevering i alle faser av etterretningsdoktrinen[10] for å kunne dele personinformasjon i alle faser i den tverrfaglige innsatsen.

Videre viser vi til Justis- og beredskapsdepartementets brev av 24. mai 2017 med høring om forslag til nytt kapittel 59 i politiregisterforskriften om behandling av opplysninger ved Nasjonalt tverretatlig analyse- og etterretningssenter (NTAES), samt direktoratets høringsuttalelse 25. august 2017.[11] Konkret foreslo Justis- og beredskapsdepartementet etableringen av et nytt politiregister med Økokrim som behandlingsansvarlig. I uttalelsen bemerket Politidirektoratet at NTAES-samarbeidet er et viktig ledd i kriminalitetsbekjempelsen på det økonomiske området, og vi imøteså i den forbindelse en avklaring av de rettslige rammene for behandlingen av opplysninger i senteret slik at senteret på en effektiv og hensiktsmessig måte kunne utnytte opplysningene til å utarbeide grunnlag til innsats mot økonomisk kriminalitet. I høringsnotatet på side 4 påpekte vi følgende:

> *Politidirektoratet ser på generelt grunnlag et behov for nærmere avklaring av når ulike typer tverretatlig samarbeid krever regulering i eget forskriftskapittel og når det kan foregå innenfor rammen av de generelle reglene i prl*[politiregisterloven]*. Som også Kripos påpeker i sin høringsuttalelse, går utviklingen mot at politiet deltar i stadig flere tverretatlige samarbeid hvor formålet nettopp er kriminalitetsbekjempelse. Det vises for eksempel til samarbeidet gjennom de såkalte a-krimsentrene hvor denne problemstillingen aktualiseres.*

Politidirektoratet oppfordrer også i denne høringsrunden at det bør utarbeides en mer generell regulering og avklaring av hjemmelsgrunnlaget og behandlingsansvaret når politiet inngår i et

[9] Justis- og beredskapsdepartementets referanse 18/2673 og Politidirektoratets høringssvar 30.05.2018 med referanse 201802191.
[10] Etterretningsfasen starter ofte med en hypotese knyttet til trusler, eksempelvis om kriminelle aktører, fenomener og grupper. Etterretningsprosessen deles i en innhentings-, analyse-/vurderings- og formidlingsfase.
[11] Justis- og beredskapsdepartementets referanse 17/1597 og Politidirektoratets referanse 201702312-12.

tverretatlig samarbeid, spesielt sett hen til de begrensningene i utleveringsadgangen som følger av taushetspliktreglene og personvernregelverket for øvrig.

Det er en forutsetning for politiets oppgaveløsning og måloppnåelse innen forebyggende, håndhevende og hjelpende virksomhet at politiet har klare og tydelige hjemler som tillater en effektiv informasjonsutveksling når politiet inngår i et tverrfaglig samarbeid med andre offentlige aktører hvis formål er å drive en effektiv kriminalitetsbekjempelse. Vi mener at tverretatlig samhandling er helt nødvendig for å kunne drive en effektiv kriminalitetsbekjempelse for eksempel innenfor arbeidslivskriminalitetsfeltet, samtidig som personvernregelverket i praksis har vist seg å være utfordrende.

Endelig vises det til høringssaken om forslag til endring i reglene om informasjonsbehandling i skatteetaten, som illustrerer utfordringene med å lage detaljerte og samtidig treffsikre/formålstjenlige regler.[12] Departementet prøver å gjøre utvidelse av utleveringshjemlene snevrest mulig, og våre kommentarer i uttalelsen viser etter vår oppfatning at departementet ikke treffer helt. Vi mener at en slik regelteknikk blir lite dynamiske og gir lite rom for å ta opp i seg den praktiske/faglige/kriminalitetsmessige utviklingen på området.

Personvern i justissektoren
Departementet viser i høringsbrevet til at personvernkommisjonen blant annet skal vurdere personvern i justissektoren, og ber om en tilbakemelding på aktuelle temaer og problemstillinger som bør prioriteres.

Politidirektoratet gjør oppmerksom på at Oslo politidistrikt i mer eller mindre grad bygger sin uttalelse på direktiv 2016/680 (heretter kalt direktivet)[13]. For en nærmere beskrivelse av direktivet vises det til Oslo politidistrikts uttalelse side 2.[14]

Behov for en evaluering og revisjon av politiregisterloven med forskrift
Både Kripos og Oslo politidistrikt mener det er et behov for en evaluering av politiregisterloven med tilhørende forskrift. Begge stiller spørsmålstegn ved hvor hensiktsmessig det er å ta utgangspunkt i en registerdefinisjon ved behandlingen av opplysninger, og peker på den forskriftsfestede plasseringen av behandlingsansvaret uten reell mulighet til å føre kontroll med behandlingen. Oslo politidistriktet illustrerer problemstillingen ved å vise til utfordringen når politiet benytter andre teknologiske plattformer, som eksempelvis Facebook og Snapchat.

I tillegg til det ovennevnte har Kripos påpekt behovet for å etablere en nedre terskel for anvendelse av enkelte bestemmelser i regelverket i tilknytning til innføringen av politiregisterlovgivningen, og viser i den forbindelse til notoritetskravet som stilles i politiregisterforskriften § 11-4 ved utlevering av offentlige tilgjengelige opplysninger til samarbeidende tjenester, der det ikke skilles mellom hvor opplysningene er hentet fra.

Oslo politidistrikt mener det bør utformes en egen bestemmelse i politiregisterloven som gjennomfører direktivets artikkel 4 om personvernprinsipper, og anfører i sin begrunnelse at en slik implementering i større grad vil bidra til harmonisering og brukervennlighet. Distriktet

[12] Finansdepartementets referanse 16/2005 og Politidirektoratets referanse 201801698-15.
[13] Det er politiregisterloven med forskrift som gjennomfører direktivet i norsk rett, se Prop. 99 L (2016–2017), *Endringer i politiregisterloven mv.* (gjennomføring av direktiv (EU) 2016/680mv.).
[14] Sistnevnte direktiv regulerer beskyttelse av fysiske personer ved behandlingen av personopplysninger for å forebygge, etterforske, avdekke eller straffeforfølge lovbrudd eller gjennomføringen av straffesanksjoner, og om fri utveksling av slike opplysninger.

stiller videre spørsmål ved hvorfor ikke alle personvernprinsippene er gjennomført i politiregisterloven, og fremhever rettferdighetsprinsippet.

Politidirektoratet har ved flere anledninger fremhevet at det er behov for en evaluering og revisjon av politiregisterloven med tilhørende forskrift med sikte på en klargjøring av bestemmelsene i lov og forskrift, herunder økt brukervennlighet. Politidirektoratet viser senest til høring om endringer i politiregisterloven og politiregisterforskriften - implementering av direktiv (EU) 2016/680, høringssvar 15. desember 2016, der vi på side 2 pekte vi på behovet for en helhetlig evaluering av politiregisterloven med forskrift. [15]

Dagens regelverk er komplisert og vanskelig å navigere i og det kan stilles spørsmål ved om et komplisert og fragmentert lovverket gir økt personvern i praksis. Særlig politiregisterforskriften er svært detaljert og fragmentarisk bygget opp. Ved utformingen av reglene ble det i stor grad tatt utgangspunkt i gjeldende registre og IKT-systemer på tidspunktet reglene ble utformet. Det er store utviklingsarbeider på gang i politiet når det gjelder digitalisering og bedre IKT-understøttelse av politiets oppgaveløsning, og det er lagt en strategi for modernisering av politiets IKT-løsninger ("Strategi for fremtidig IKT-funksjon i politiet"). Dette vil blant annet medføre at informasjon vil struktureres på en annen måte enn i de gamle løsningene og at de fremtidige IKT-løsningene bygges opp på nye måter. Etter Politidirektoratets oppfatning er gjeldende politiregisterforskrift bygget på en "analog" tankegang og er krevende å anvende i dette perspektivet.

Offentlig tilgjengelig informasjon og politiansattes personvern
Agder politidistrikt og Kripos trekker blant annet frem aktuelle problemstillinger som oppstår når informasjon gjøres tilgjengelig på internett gjennom åpne kilder mv., og opp mot offentlige ansattes personvern. Kripos peker blant annet på at det er vanskelig å ha tilstrekkelig kontroll med bruken av disse opplysningene og foreslår på denne bakgrunn at det bør foretas en gjennomgang av offentlige etaters adgang til å behandle opplysninger fra åpne kilder generelt og politiets adgang til å behandle slike opplysninger spesielt[16].

Politidirektoratet er enig i dette. Direktoratet har i tilknytning til behandlingen av ny personopplysningslov spilt inn behovet for en avklaring av innsynsretten etter offentleglova og personopplysingslova. Det vises til forslag til lovvedtak og stortingsvedtak (Prop. 65 LS (2017–2018))[17] der departementet i punkt 2.3.1 redegjør for rammene for arbeidet med ny personopplysningslov, og uttaler på side 13 at "[f]orholdet mellom offentleglova og personopplysningsloven vil bli nærmere vurdert i sammenheng med arbeidet med evalueringen av offentleglova".

Departementet viser på side 6 i proposisjonen til tilbakemeldinger fra flere høringsinstanser, der det pekes på at det er et motsetningsforhold mellom hensynene offentleglova skal ivareta og hensynet til skjerming av personopplysninger, som personopplysningsregelverket er utviklet for å styrke.

[15] Politidirektoratets referanse: 201604312, Justis- og beredskapsdepartementets referanse: 16/6645.
[16] Kripos viser i sin uttalelse til sak om Etterretningsbataljonens behandling av opplysninger om journalister, jf. Datatilsynets referanse 14/00062, hvor Forsvaret ble pålagt å betale 75 000 kroner i overtredelsesgebyr på grunn av manglende behandlingsgrunnlag i daværende personopplysningslov § 11 jf. § 8. Opplysningene var hentet fra åpne kilder og inneholdt opplysninger om publiserte nyhetsartikler, fødselsår, bostedsadresse og registreringer i Brønnøysundregistrene.
[17] Lov om behandlingen av personopplysninger (personopplysningsloven) og samtykke til deltakelse i en beslutning i EØS-komiteen om innlemmelse av forordning (EU) nr. 2016/679 (generell personvernforordning) i EØS-avtalen.

I forlengelsen av dette har det i senere tid oppstått nye problemstillinger knyttet til forholdet mellom offentlige ansattes personvern og rett til innsyn i personalinformasjon hos ansatte i politiet. Den økte digitaliseringen av samfunnet medfører at informasjon enkelt kan spres. Faren for digital spredning av dokumenter/opplysninger og koblingen opp mot andre tilgjengelige opplysninger i åpne kilder kan innebære at det ikke er tilstrekkelig å anonymisere dokumenter. Ved krav om innsyn etter offentleglova i slike saker må det foretas vanskelige avvenninger av allmennhetens rett til innsyn og hensynet til den ansattes personvern. Offentleglova gir ikke en generell adgang til å unnta personalmapper eller personalrelatert informasjon fra innsyn, og det må foretas en konkret og individuell vurdering i hvert enkelt tilfelle. Saker politidirektoratet har hatt til behandling viser at regelverket kan være vanskelig å praktisere på dette området, herunder hvor grensene for innsyn skal trekkes. Konkret pekes det på utfordringen med at man i den konkrete innsynsvurderingen ofte ikke kjenner til hvilke opplysninger som er tilgjengelige for mottaker fra *andre kilder* (såkalt koblingsfare). Direktoratet viser til blant annet offl. § 24 tredje ledd som gir en rett til å unnta opplysninger fra innsyn dersom det er "påkravd fordi innsyn ville utsetje enkeltpersonar for fare…", men på grunn av bestemmelsens ordlyd og krav til dokumentasjon antas det at bestemmelsen ikke alene løser dagens utfordringer. Politidirektoratet vil særlig fremheve at det for politiets ansatte også vil være et spørsmål om ansattes sikkerhet i tillegg til personvern, noe offl. § 24 tredje ledd generelt er ment å fange opp.

Politidirektoratet viser til og fastholder sin tidligere uttalelse knyttet til behovet for en avklaring mellom rett til innsyn etter offentleglova på den ene siden og personopplysningsloven og politiregisterloven på den andre siden, og mener at personvernkommisjonen bør foreta en slik evaluering av regelverket.

<u>Behandling av særlige kategorier personopplysninger som den registrerte har offentliggjort</u>
Oslo politidistrikt knytter sine merknader til direktivets artikkel 10 bokstav c som hjemler en adgang til å behandle særlige typer kategorier personopplysninger på visse strenge vilkår og når behandlingen gjelder opplysninger som det er åpenbart at den registrerte har offentliggjort. Distriktet mener at direktivets artikkel 10 bokstav c bør innføres i norsk rett. Videre fremholder distriktet at kommisjonen bør drøfte grensene for politiets adgang til å bruke opplysninger som den registrerte selv har offentliggjort. Bestemmelsen er gjennomført i medlemslandene, og Oslo politidistrikt viser på side 4 i sin uttalelse til hvorfor bokstav c ikke er gjennomført i norsk rett. Politidirektoratet ber departementet vurdere distriktets innspill.

<u>Bruk av ny teknologi og metoder</u>
Politidirektoratet er enige i de høringsinstansene som har gitt innspill til direktoratet at det er avgjørende at politiet har tilgang relevant informasjon og har muligheten til å sammenstille disse. Kripos og Oslo politidistrikt fremholder på denne bakgrunn at personvernkommisjonen bør prioritere å se nærmere på politiets behov og adgang til å ta i bruk ny teknologi som "Big data", kunstig intelligens, profilering. Politidirektoratet tiltrer merknadene til Kripos og Oslo politidistrikt, og legger til at muligheten til å nyttiggjøre seg av ny teknologi og metoder som ikke i for stor utstrekning begrenses av personvernregelverket, er en forutsetning for at politiet som sådan skal kunne løse sitt samfunnsoppdrag.

Kripos fremholder i sin uttalelse:

> *Det vil ofte være avgjørende å ha tilgang til store mengder opplysninger for å kunne benytte seg av maskinlæring til å se mønstre, profilere eller utvikle systemer for*

automatiserte avgjørelsers.[18] *Analyse av store mengder opplysninger kan være et instrument for å eksempelvis kunne planlegge bruken av ressurser, eller som et seleksjonsverktøy for å kunne utføre en mer målrettet kontroll. For eksempel har politiet innført et logganalyseverktøy for å kunne foreta en mer målrettet kontroll med politiets bruk av egne registre. Et annet eksempel er bruken av ANPR*[19] *som gjør at politiet ved bruk av kamera som automatisk leser skiltene på biler som passerer patruljen, sjekkes opp mot opplysninger fra Autosys og etterlysningsregisteret, kan foreta en mer målrettet kontroll av kjøretøy. Det bemerkes for ordens skyld at slike analyser kan være vel så viktige for å avdekke tendenser og fenomener, og således ikke utelukkende* med virkning for enkeltpersoner. Dette er et tema som har stor nyhetsinteresse, og det har vært flere oppslag om f.eks. leverandøren Palantirs inntreden i offentlige etater som tolletaten og politiet.

Oslo politidistrikt vurderer fordelene med bruk av ny teknologi samtidig som det peker på hvilket inngrep ny teknologi kan innebære i personvernet, og kommer til at personvernkommisjonens arbeid med dette kan bidra til å finne et riktig balansepunkt mellom grunnleggende interesser.

Oslo politidistrikt mener blant annet at direktivet 2016/680 artikkel 11 bør gjennomføres i norsk rett i tilknytning til automatiserte avgjørelser og profilering. Distriktet opplyser om at bestemmelsen ikke er gjennomført i Norge, noe som skal ha vært tilsiktet ut fra lovforarbeidene til art. 11, men stiller spørsmål ved om dette er fyllestgjørende.

Politidirektoratet viser til Kripos og Oslo politidistrikt høringsuttalelse som støttes i sin helhet.

Datalagringsdirektivet
Kripos viser i sin uttalelse til at regjeringen, som en følge av at datalagringsdirektivet ble erklært ugyldig av EU-domstolen i 2014, uttalte at de skulle komme tilbake til et lovforslag om datalagring, noe Kripos peker på har uteblitt. Det vises til side 4 i Kripos uttalelse der de mener det er av interesse å få belyst en mer prinsipiell tilnærming til lagring av opplysninger om alle borgere for å kunne plukke ut de få, på nærmere bestemte vilkår. Politidirektoratet støtter Kripos sine merknader.

Identitetsforvaltning, politiets tilgang til opplysninger uten bruk av tvangsmidler og vandelsinstituttet
Det vises til Kripos høringsuttalelse, der de på side 3 peker på tre områder som bør utredes nærmere og således inngå i mandatet til personvernkommisjonen. Politidirektoratet er enige i at dette er tre områder det er behov for å utrede nærmere, og ber om at dette vurderes av departementet.

Bruk av digitale løsninger og rettighetene til brukere av sosiale medier
Bruk av digitale løsninger og rettighetene til brukere av sosiale medier
Departementet viser i høringsbrevet til at kommisjonen skal se på hvordan personvernet kan sikres ved økt bruk av digitale løsninger, herunder rettighetene til brukere av sosiale medier.

[18] Artikkel 11 i EU-direktiv 2016/680 omhandler automatiserte avgjørelser. Bestemmelsen er ikke gjennomført i norsk rett fordi "... det i Norge ikke er ordninger der individuelle avgjørelser som er av betydning for den det gjelder utelukkende er basert på automatisk behandling", jf. Prop. 99 L punkt 4.3.1. Kripos anbefaler at behovet for bestemmelsen revurderes.
[19] Automated number plate recognition.

Kripos og Oslo politidistrikt mener andre temaer bør gis prioritet, og fremholder blant annet at ivaretakelse av personvernet til brukere av sosiale medier og andre digitale løsninger er gjennomregulert i ny personopplysningslov og ny personvernforordning.

Etter Politidirektoratets oppfatning er det behov for å se på hvordan og i hvilken grad teknologiutviklingen og internett bidrar til å forsterke omfanget av integritetskrenkende kriminalitet, og hvordan dette i seg selv utfordrer personvernet. Vi imøteser at dette bør bli en del av det uttalte ønsket om å se på økt bruk av digitale løsninger, herunder rettighetene til brukere av sosiale medier.

Barns personvern og tiltak for å styrke dette
Departementet ber i høringsbrevet om høringsinstansenes tilbakemelding på tiltak som kan styrke barns personvern knyttet til kommisjonens særlige oppdrag om å vurdere tilstanden for barns personvern.

Kripos og Oslo politidistrikt mener at personvern i justissektoren bør prioriteres fremfor en vurdering av tilstanden til barns personvern idet de viser til at den forrige personvernkommisjonen i sin utredning NOU 2009: 1 så særskilt på personvern og media, barn og unge, i arbeidslivet, helsesektoren og i transport og kommunikasjonssektoren, samt spørsmålet om organisering av personvernmyndighetene og grunnlovsfesting av personvernet.

Politidirektoratet ser viktigheten av at det fokuseres på tilstanden til barns personvern, men tiltrer merknadene til Kripos og Oslo politidistrikt. Politidirektoratet bemerker at enkelte partier under behandlingen av representantforslaget var opptatt av at en sammenslåing av en gjennomgang av tilstanden til barns personvern med det opprinnelige mandatet til personvernkommisjonen ikke måtte flyttet fokuset bort fra en vurdering av tilstanden til barns personvern. Områder representantforslaget særlig rettet søkelyset mot var personvernets betydning knyttet til registrering og overføring av personlige opplysninger, kameraovervåking, samt sosiale medier og GPS-sporing i barnehage og skoler. Politidirektoratet stiller spørsmål ved om dette er den mest hensiktsmessige inndeling av personvernkommisjonens mandat og oppdrag sett hen til anbefalingen om at mandatet ikke bør utformes for bredt.

Med hilsen

Håkon Skulstad
assisterende Politidirektør

Olav Kjetil Moe
fungerende seksjonssjef

Dokumentet er elektronisk godkjent uten signatur.

Saksbehandler:
- Alexander Fotland Iversen

Vedlagt følger høringsinstansenes innspill:
- Kripos høringsinnspill 13.08.2018
- Oslo politidistrikt 14.08.2018
- Agder politidistrikt 10.08.2018