



POLITIET
POLITIDIREKTORATET

Justis- og beredskapsdepartementet

Postboks 8005 Dep
0030 OSLO

NATIONAL POLICE DIRECTORATE

Deres referanse:
18/3955

Vår referanse:
201803252-11 008

Sted, Dato
Oslo, 03.10.2018

HØRINGSSVAR - PERSONVERNKOMMISSJON - 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, Kripes og Økokrim. Sistnevnte særorgan hadde ingen merknader til høringen.

I forbindelse med at regjeringen skal nedsette en personvernkommissjon som skal vurdere personvernets stilling i Norge ber departementet om innspill til utforming av personvernkommissjonens mandat. Personvernkommissjonen 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 personvernkommissjon 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 personvernkommissjon, 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 *personopplysningsvern* 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

Politi-loven § 2 stadfester at politiets primæroppgave er å bekjempe kriminalitet. Dette kan omtales som kriminalitetsbekjempelsesfunksjonen, som tar opp i seg politiets oppgaver innen forebygging, etterforskning og strafforfølgning. 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 begrensninger 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 personvern hensyn. 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 rapport³ 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 offentlige 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 kontrollatene, 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 (forslag 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 (forslag 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 etterretningsdoktrinen¹⁰ 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 høringsaken 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 spesielt¹⁶.

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 personopplysningslova. 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 avveininger 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 utsette 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.

Behandling av særlige kategorier personopplysninger som den registrerte har offentliggjort

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.

Bruk av ny teknologi og metoder

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 avgjørelser.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 ANPR¹⁹ 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 ivaretagelse 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 flytte 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



POLITIET

Politidirektoratet

Postboks 2090 Vika
0125 OSLO

AGDER POLITIDISTRIKT

Deres referanse:

Vår referanse:
201803662-3 722Sted, Dato
Kristiansand, 10.08.2018**AGDER POLITIDISTRIKTS INNSPILL TIL PERSONVERNKOMMISSJONENS MANDAT**

Det vises til høringsbrev vedrørende innspill til Personvernkommissjons mandat, datert 23. juli.

Når det gjelder hvordan personvernet kan sikres ved økt bruk av digitale løsninger, herunder rettighetene til brukere av sosiale medier, har man følgende innspill til mandatet:

- Man bør se på muligheten for å etablere en helhetlig elektronisk sikkerhetsklareringsprosess; dagens papirbaserte løsning er både ressurskrevende, ineffektiv og har utfordringer knyttet til personvern.
- Man bør se på muligheter for å benytte løsninger som Altinn til også å omfatte kommunikasjon av ulik art med offentlige instanser, utover hva som allerede er etablert. For å ivareta personvernet på en bedre måte enn i dag, vil kommunikasjon via Altinn sørge for en sikrere verifikasjon av den som faktisk kommuniserer med aktuell instans. Verifikasjon er også av vesentlig betydning for personvernet ved kommunikasjon via ulike sambandsmedier.
- Man bør se på ulike utfordringer knyttet til stadig større utstrekning i bruken av sosiale medier, herunder innsamling av personopplysninger inn mot Big Data og målrettet kommunikasjon.

Hva angår det særlige oppdraget om å vurdere tilstanden for barns personvern og tiltak for å styrke dette, har man følgende innspill til mandatet:

- Man bør se på tilfeller hvor ulike hensyn er motstridende, spesielt knyttet til sletting av opplysninger. I dag risikerer man at opplysninger som kan bli nødvendige i saker om tapt barndom, blir slettet, og ikke sperret.

AGDER POLITIDISTRIKT

Da mandatet for øvrig er åpent, tillater man seg å komme med følgende innspill:

- Man bør se på tilfeller hvor det kan være nødvendig å skjerme opplysninger knyttet til ansatte, som av ulike hensyn ikke bør tilflyte offentligheten, i større grad. Dette kan være relevant for å ivareta personvernet til både ansatte innen særlig utsatte sektorer/stillinger, eksempelvis politioperativt personell, samt personer i den ansattes nærmeste familie.
- Man bør se på muligheter for, og krav om gjenbruk av personopplysninger/data. Gjenbruk vil sannsynligvis redusere risiko for feil *ved* opplysningene og *ved behandlingen* av disse.
- Man bør ta inn over seg utviklingen i retning av mer samarbeid mellom ulike aktører, herunder tverretattlig. Eksempelvis har politiet, kommuner, helse- og skolevesenet behov for større grad av informasjonsutveksling av personopplysninger som én eller flere av aktørene har, men hindres ofte av at de er underlagt ulikt regelverk knyttet til blant annet taushetsplikt.

Med hilsen

Arne Sundvoll
Visepolitimester

Dokumentet er elektronisk godkjent uten signatur.

Saksbehandler:

Hans Tangen
Seniorrådgiver



POLITIET
KRIPOS

Politidirektoratet

politidirektoratet@politiet.no

NCIS Norway

Deres referanse:

Vår referanse:

Sted, dato

2018/00727

Oslo, 13.08.2018

PERSONVERNKOMMISSJONEN – INNSPILL TIL MANDAT

Det vises til Politidirektoratets e-post av 23. juli 2018 vedrørende innspill til mandat til Personvernkommissjonen med svarfrist til direktoratet 11. august 2018. Kripos har etter anmodning fått innvilget utsatt svarfrist til 13. august.

Innledningsvis bemerkes det at det er positivt at departementet tar et slikt initiativ, da det er mange personvernrettslige problemstillinger som kan og bør løftes. For at kommisjonen skal ha anledning til å gå i dybden på noen av vår tids viktigste problemstillinger, er det imidlertid viktig at kommisjonens mandat ikke utformes for bredt.

Kommisjonen skal ifølge Jeløya-plattformen og Stortingets anmodningsvedtak nr. 588 særlig se på personvern i justissektoren, hvordan personvernet kan sikres ved økt bruk av digitale løsninger, herunder rettighetene til brukere av sosiale medier, og tiltak for å sikre barns personvern. Den forrige personvernkommissjonen så i sin utredning NOU 2009: 1 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. Personvern berører alle individer og alle sektorer, og det vil derfor være nødvendig å foreta gode prioriteringer ved utvelgelsen av temaer. Sett hen til tidligere behandlede områder støtter Kripos en prioritering av personvern i justissektoren. Nedenfor følger Kripos' innspill.

Offentlige etaters behandling av personopplysninger

Offentlige etater behandler store mengder personopplysninger om befolkningen. Den teknologiske utviklingen medfører at det lagres opplysninger i større omfang enn tidligere, opplysningene kan lettere sammenstilles, og det er enkelt å gi tilgang til opplysninger. Det er videre en forventning om at forvaltningen skal effektiviseres gjennom bruk av digitale verktøy, at opplysninger skal gjøres tilgjengelig for såkalt viderebruk, og en forventning om økt samhandling mellom offentlige etater samt mellom offentlige etater og private aktører.

Behandling av personopplysninger i regi av det offentlige er som hovedregel lovregulert. I mange tilfeller behandles opplysningene derfor uten et samtykke fra den registrerte og uten

Kripos/

Post: Pb. 2094 Vikla, 0125 Oslo
Besøk: Brynsalléen 6, 0667 Oslo
www.polti.no/kripos

Telefon: (+47) 23 20 80 00
Telefaks: (+47) 23 20 88 80
E-post: kripos@politiet.no

Org. nr: 974 760 827

at den registrerte har fått informasjon om behandlingen. Videre har borgeren ofte en plikt til å gi opplysninger, alternativt er behandlingen av opplysninger en forutsetning for å kunne tildele en ytelse til den registrerte. I motsetning til private aktører, kan offentlige etater fatte vedtak og iverksette tiltak som kan få store konsekvenser for den registrertes rettsstilling, og den registrerte kan ikke reservere seg mot denne behandlingen, ei heller velge en annen "leverandør" for å oppnå det samme. Særtrekkene ved behandling av personopplysninger i det offentlige gjør at dette er et interessant område for kommisjonen.

I stortingsmeldingen *Digital agenda for Norge* beskrives regjeringens hovedmål og prioriteringer i IKT-politikken. Et av prinsippene som løftes frem for å sikre en brukerrettet og effektiv forvaltning er at "[i]nformasjon til forvaltningen skal leveres kun én gang", nærmere bestemt at "[f]orvaltningen skal gjenbruke informasjon i stedet for å spørre brukerne på nytt om forhold de allerede har opplyst"¹. Dette har opplagt en mulig effektiviseringsgevinst i seg, men kan også være utfordrende opp mot prinsipper om at den enkelte selv skal ha kontroll på hvilke opplysninger som behandles, av hvem og til hvilke formål, samt blant annet kravene til kvalitet og korrekthet, da opplysningene kan endre seg over tid. Økt samhandling, gjenbruk av opplysninger og digitalisering krever en økt bevissthet om hvordan hensynet til personvern kan ivaretas på en tilfredsstillende måte.

I forlengelsen av dette bemerker Kripos at økt samhandling mellom offentlige etater, med ulike regelsett som regulerer behandlingen, kan medføre et juridisk landskap som det er vanskelig å navigere i. 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.

Offentlige etaters behandling av personopplysninger, herunder utveksling av opplysninger mellom offentlige etater, kan med fordel utredes. Det kan videre 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. Det vises for eksempel til Finansdepartementets høringsnotat av 24. mai 2018 om adgang for Skatteetaten og Tolletaten til å bruke personopplysninger ved utvikling og testing av IT-systemer.²

En rekke lovforslag de siste årene har hatt betydning for det offentliges anledning til å behandle personopplysninger om borgerne i Norge. Det kan reises spørsmål om personvernkonsekvensene ved enkelte lovforslag har vært godt nok utredet. Det vises i denne sammenheng til blant annet NOU 2018: 7 Statistikklovutvalget, hvor utredningen av personvernkonsekvensene av lovforslaget er mangelfull. Etter Kripos' syn bør det vurderes om personvernkonsekvenser av lov- og forskriftsforslag utredes godt nok, og hvilke tiltak som ev. kan settes i verk for å sikre at personvernkonsekvenser utredes tilfredsstillende.

¹ St. 27 (2015-2016) del 2 punkt 7.

² Departementets saksnummer 18/1077.

Personvern i justissektoren

Det er en rekke særskilte personvernrettslige problemstillinger i justissektoren. Et aspekt gjelder politiet som innehaver av flere roller og dertil hørende regelverk, for eksempel politiet som 1. linjeinstans i utlendingsforvaltningen og politiet som politimyndighet. Utover dette vil Kripos avgrense seg til å nevne noen temaer som kan være av interesse i det følgende.

Identitetsforvaltning

Kripos ser et behov for å avstemme ulike regelverk opp mot bestemmelsene om identitetsfastsettelse. Per dags dato foreligger ikke en enhetlig og sektorovergripende måte å fastsette entydig identitet på, ei heller en enhetlig identitetsforvaltning utover Folkeregisteret, som har kjente mangler.

Samfunnsutviklingen medfører et klart behov for å fastsette eller bekrefte identitet på en entydig måte ved å kunne knytte personers navn og fødselsnummer mot en persons biometri, og at disse opplysningene er tilgjengelige for de som har tjenstlig/tjenestemessig behov for slike opplysninger. Samtidig er det viktig å utrede hvordan biometri kan søkes og returnere svar uten at selve biometrien deles, eller må lagres flere steder. For samfunnet vil dette kunne avhjelpe ID-håndtering knyttet til hvilke rettigheter og plikter personer i samfunnet har krav på, for eksempel knyttet til skatt, førerkort og banktjenester. For politiet er det meget viktig å kunne fastsette rett ID på personer tidligst mulig i saksbehandlingen. Dette for å sikre at personene vi jobber med ikke forsøker å unndra seg etterlysninger eller andre forhold knyttet til andre brukte identiteter. I tillegg er det for politiet et sikkerhetsselement knyttet til å vite hvem vi jobber med, under hele prosessen.

Politiets tilgang til opplysninger – uten bruk av tvangshjemler

Ny personopplysningslov, som gjennomfører EUs personvernforordning i norsk lov, trådte i kraft 20. juli 2018. I den forbindelse opplever Kripos at politiets informasjonsinnhenting fra private parter i forbindelse med straffesaker er vanskeliggjort. Det bør utredes i hvilken grad ikrafttreddelsen av personvernforordningen påvirker politiets evne til å oppklare kriminalitet. Et eksempel er bruken av samtykke til innhenting av trafikkdata, hvor en leverandør er av den oppfatning at samtykke ikke lenger er et gyldig behandlingsgrunnlag etter ikrafttreddelsen av ny personopplysningslov. Et eksempel utenfor straffesak gjelder innhenting av tannjournaler fra tannlege i forbindelse med identifiseringsarbeid, hvor formålet med undersøkelsen er å fastsette sikker identitet på avdød person. Kripos understreker viktigheten av at politiet har adgang til å innhente opplysninger til bruk til politimessige formål, utover innhenting av opplysninger ved bruk av tvangshjemler.

Vandelsinstituttet

Ved ikrafttreddelsen av politiregisterloven med forskrift 1. juli 2014 ble bestemmelsene om vandelskontroll og attester samlet ett sted. Det har de siste tiårene vært en økt satsing på bruken av vandelsinstituttet som tiltak for å unngå at personer som kan være uskikket i nærmere definerte roller og stillinger skal få slike verv og stillinger. Innføring av hjemmel for å innhente politiattest er imidlertid et svært begrenset virkemiddel, og Kripos ser ofte at straffebestemmelsene som er positivt avgrenset gir et til dels svært mangelfullt bilde av skikketheten til den omspurte. Som en følge av dette innhentes det ofte supplerende opplysninger som belyser en persons vandel og skikkethet, hvilket innebærer ytterligere inngrep i personvernet, samt kan medføre en ulik praksis. I tillegg kommer vandelskontroll i form av akkreditering, f.eks. akkreditering av flyplasspersonell som har avdekket flere vanskelige juridiske problemstillinger. Til dette formål innhentes det opplysninger om ansatte

som det ikke gis rett til innsyn i, og kan føre til at ansatte som har utført en upåklagelig jobb i 15 år mister adgangskortet på dagen, uten noen nærmere begrunnelse for hvorfor. Videre utfører NSM personellkontroll etter sikkerhetsloven, hvor det i forskrift til sikkerhetsloven foreslås at NSM skal kunne innhente opplysninger fra "politiets registre" til bruk i slik kontroll, uten noen nærmere avgrensning.³ Også her er det utfordringer knyttet til den registrertes rettigheter, samt behovet for å verne om opplysninger av hensyn til for eksempel etterforskningen.

Datalagringsdirektivet

Datalagringsdirektivet ble vedtatt i EU i 2006, og i Stortinget i april 2011. Direktivet ble erklært ugyldig av EU-domstolen i 2014, hvorpå det norske lovforslaget ble lagt på is. Regjeringen skulle senere komme tilbake til et lovforslag om datalagring, men dette har uteblitt. Kripos påpekte i sitt hørings svar i 2010 at det ikke var foretatt en kartlegging av politi og påtalemyndighetens behov for denne type bevis, noe som vanskeliggjorde en balansert avveining mellom hensyn til kriminalitetsbekjempelse og personvern. Denne avveiningen er like relevant i dag, og behovet for datalagring er like viktig for politiet og påtalemyndigheten som det var da.⁴ En prinsipiell tilnærming til lagring av opplysninger om alle borgere for å kunne plukke ut de få, på nærmere bestemte vilkår, er av interesse å få belyst. Denne problemstillingen er videre interessant sett i lys av forslaget om digitalt grenseforsvar, jf. Lysne II-utvalget. Også dette forslaget skapte stor debatt, og et av innspillene fra Kripos var at sentrale problemstillinger ikke var drøftet, herunder håndtering av overskuddsinformasjon og forholdet til politiet.

Ny teknologi og metoder

Et fyndord er begrepet "big data", som brukes om svært mange ulike behandlinger. Essensen i det, nemlig at store mengder opplysninger sammenstilles, for derigjennom å kunne danne grunnlag for ulike former for analyser, profilering, slutninger og kunnskapsgrunnlag, er utvilsomt interessant i et personvernperspektiv.

Bakgrunnsbildet med forventninger om effektivisering og best mulig bruk av begrensede offentlige ressurser, taler for at politiet og offentlige etater mer generelt skal ta i bruk nye verktøy som hjelpemidler for å utføre samfunnsoppdraget på en effektiv og treffsikker måte.

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 avgjørelser⁵. 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 ANPR⁶ som gjør at politiet ved bruk av kamera som automatisk leser skiltene på biler som passerer patroljen, 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

³ Høringsnotat – forslag til forskrifter til ny sikkerhetslov av 2. juli 2018. Høringsfrist 1. oktober 2018.

⁴ Se også brev fra Riksadvokaten til Justis- og beredskapsdepartementet av 26. mai 2014, jf. departementets referanse 14/2315.

⁵ 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.

⁶ Automated number plate recognition.

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.

Offentlig tilgjengelige opplysninger

Digitaliseringen medfører at en stor mengde personopplysninger er tilgjengelig på Internett gjennom åpne-, delvis åpne og mer lukkede kilder. Dette kan være nyhetssaker som er publisert på digitale medier, blogger, offentlige dokumenter som er gjort tilgjengelig gjennom postjournaler eller sider som www.mimesbronn.no, sosiale medier, mv. Disse opplysningene kan med relativt enkle virkemidler gjenbrukes av offentlige og private aktører for andre formål enn det opprinnelige, og det er vanskelig å ha kontroll med bruken av disse opplysningene. Spørsmålet om hva som er formålet med innhenting er dessuten irrelevant etter eksempelvis offentleglova. Loven åpner for eksempel for at enhver kan få tilgang til store mengder opplysninger om ansatte i offentlige sektor, som til dels er av nokså privat karakter, og som mange i alle fall ikke har et ønske om at skal ligge tilgjengelig ved ethvert Google-søk. I lys av den teknologiske utviklingen bør det foretas en gjennomgang av anledningen til behandle opplysninger fra åpne kilder generelt og politiets adgang til å behandle slike opplysninger spesielt.⁷ Det bemerkes videre at det synes å være et behov for å se nærmere på avveiningen mellom personvern og offentlighet opp mot offentleglova.

Gjennomgang av politiregisterlovgivningen

Kripos har ved flere anledninger løftet behovet for en evaluering av politiregisterloven med forskrift. Loven trådte i kraft 1. juli 2014. Det kan for eksempel stilles spørsmål ved hvor hensiktsmessig det er å ta utgangspunkt i en registerdefinisjon ved behandling av opplysninger sett hen til den teknologiske utviklingen. Enn videre har Kripos gitt uttrykk for en bekymring knyttet til plassering av behandlingsansvar uten reell kontroll med behandlingen. Eksempelvis kan ikke Kripos som behandlingsansvarlig for arrestjournal alene beslutte og prioritere nødvendige endringer for å etterleve lovkravene. En forskriftsfestet plassering av behandlingsansvaret kan i noen tilfeller medføre et ansvar uten tilhørende myndighet, noe som igjen kan medføre negative konsekvenser for personvernet.

I forbindelse med Innføring av politiregisterlovgivningen har Kripos ved påpekt behovet for å etablere en nedre terskel for anvendelse av enkelte bestemmelser i regelverket. Et kjent eksempel er utlevering av offentlige tilgjengelige opplysninger til samarbeidende tjenester, hvor det etter politiregisterforskriften § 11-4 er et krav om notoritet uavhengig av hvor opplysningene er hentet fra. Det fremstår for eksempel som lite hensiktsmessig at Kripos, ved utlevering av opplysninger om hvem som eier en gitt bil til finske myndigheter, må etterleve krav til notoritet når de samme opplysningene er offentlige tilgjengelige gjennom bruk av SMS-tjeneste for enhver – uten krav til logging av hvem som har bedt om hvilke opplysninger.

Kripos har videre spilt inn et behov for en helhetlig gjennomgang av reglene for opptak og registrering av DNA til Riksadvokaten.

⁷ Se også 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.

Bruk av digitale løsninger og rettighetene til brukere av sosiale medier

Ivaretagelse av personvernet til brukere av sosiale medier og andre digitale løsninger er gjennomregulert i ny personopplysningslov og ny personvernforordning. Etter Kripos' syn bør derfor andre temaer gis prioritet.

Innspill til sammensetning av kommisjonen

Kommisjonen bør ha en bred sammensetning hvor blant annet teknologer og samfunnsvitere bør ha plass i tillegg til jurister. Det anses videre nødvendig at flere representanter fra justissektoren deltar i kommisjonen, herunder personer med politifaglig bakgrunn.

Med hilsen



Ketil Haukaas

Saksbehandler Mari Hersoug Nedberg

seniorrådgiver

Telefon: +47 23 20 80 28



POLITIET

Politidirektoratet
Postboks 8051 Dep.
0031 OSLO

OSLO POLITIDISTRIKT

Deres referanse:

Vår referanse:
201809192-2 008

Sted, Dato
, 14.08.2018

HØRINGSSVAR OM MANDAT TIL PERSONVERNKOMMISSJON

Vi viser til høringsbrev av 11. juli 2018. Det er i høringsbrevet pekt på at regjeringen skal nedsette en personvernkommissjon som skal vurdere personvernets stilling i Norge.

Personvernkommissjonen skal i følge Jeløya-plattformen blant annet se på; "personvern i justissektoren, og hvordan personvernet kan sikres ved økt bruk av digitale løsninger, herunder rettigheter til brukere av sosiale medier. Mandatet skal også inkludere et særlig oppdrag om å vurdere tilstanden for barns personvern og tiltak for å styrke dette ...". Det er pekt på at mandatet for øvrig er åpent, og at det for eksempel kan gis innspill til bestemte områder, temaer eller spørsmål som personvernkommissjonen bør se nærmere på.

Generelt

Vi er positive til etablering av en ny personvernkommissjon, og mener det er viktig at kommisjonen foretar en gjennomgang av personvernets tilstand.

Vi mener mandatet bør ses i sammenheng med nytt personopplysningsregelverk, og spesielt forordning 2016/670 (heretter personvernforordningen) og direktiv 2016/680 (heretter LED¹). Vi mener i tillegg at mandatet bør ses i sammenheng med utredningen personvernkommissjonen gjorde i 2009.² I 2009 så personvernkommissjonen 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. Ut fra de særskilte områder som ble behandlet i 2009 støtter vi prioriteringen av personvern i justissektoren.

Vi setter imidlertid spørsmåltegn ved hvorfor økt bruk av digitale tjenester og sosiale medier skal prioriteres. Bruk av slike kommersielle tjenester er allerede regulert av personvernforordningen, og det er et begrenset handlingsrom til å innføre nasjonale regler på dette feltet.

¹ Artikkel 29 gruppen bruker forkortelsen LED på direktivet i sin uttalelse WP 258. Det står for Law Enforcement Directive.

² NOU: 2009: 1 Individ og integritet.

OSLO POLITIDISTRIKT

Om LED og økt krav til harmonisering

Personopplysningsvernet har utviklet seg til å bli en moderne og selvstendig rettighet, og rettsutviklingen på dette området skjer i stor grad i EU. Dette gjelder både gjennom lovgivningen, praksis og tolkninger fra sentrale organer. Vi trekker særlig frem rettspraksis fra EU-domstolen og uttalelser fra Artikkel 29 gruppen (EU-kommisjonens ekspertorgan på personvern). Artikkel 29 gruppen har hatt et stort aktivitetsnivå og har kommet med en rekke uttalelser og tolkninger, som igjen har hatt stor innflytelse på forståelsen av personvernordningens grunnleggende begreper og tankegang. Artikkel 29 gruppen er nå erstattet med Personvernrådet, som både har oppgaver etter personvernforordningen og LED. Personvernrådet må forventes å få stor betydning for forståelsen og praktiseringen av LED.

LED må kunne sies å ha kommet noe i skyggen av personvernforordningen, men direktivet har vesentlig betydning for borgernes rettsikkerhet og personopplysningsvern. Direktivet regulerer et område hvor det må foretas vanskelige balansevalg mellom hensynet til kriminalitetsbekjempelse på den ene siden og hensynet til den enkeltes personopplysningsvern på den andre siden. Balanseringen av interesser foretas spesielt gjennom regler som setter begrensninger i adgangen til å behandle personopplysninger, samt ved rettighetsbestemmelser. Ved å benytte seg av et direktiv fremfor en forordning gis medlemsstatene også et noe større nasjonalt handlingsrom til å fastsette egne regler. Et slikt handlingsrom tar hensyn til kulturelle, rettslige og historiske forskjeller mellom medlemslandene. Det påpekes imidlertid at LED innebærer nokså strenge krav til harmonisering.³ Det er politiregisterloven med forskrift som gjennomfører LED i norsk rett.

Justissektoren

Behov for gjennomgang av regelverket

Det er mange ulike personvernrettslige problemstillinger som gjør seg gjeldende i justissektoren. Vi vil i det følgende fokusere på de rammer som følger av LED og det handlingsrom Norge har til å utforme nasjonale regler.

Politiregisterloven med forskrift

Vi mener det er behov for en evaluering av politiregisterloven med forskrift. Vi mener det kan settes spørsmålstegn ved om regelverket er tilstrekkelig fleksibelt og teknologinøytralt sett hen til den teknologiske utviklingen. Det kan for eksempel stilles spørsmål ved hvor hensiktsmessig det er å ta utgangspunkt i en registerdefinisjon ved behandling av opplysninger. En annen utfordring er registerfokus og den forskriftfestede plassering av behandlingsansvaret når politiet tar i bruk nye teknologiske plattformer som Facebook og Snapchat. Vi viser i den forbindelse til EU-domstolens avgjørelse om felles behandlingsansvar mellom Facebook og en tysk utdanningsinstitusjon.⁴

Personvernprinsipper

Etter vår vurdering er artikkel 4 den mest sentrale bestemmelsen i direktivet. Ikke bare har prinsippene betydning ved tolking av de øvrige bestemmelsene i direktivet, de har også normativ kraft i seg selv. Praktiseringen av prinsippene er dessuten viktig for å sikre harmonisering av regelverket i medlemsstatene. Prinsippene er dessuten teknologinøytrale og har vist fleksibilitet med tanke på teknologisk utvikling. Det foreligger tolkninger av prinsippene innenfor rettshåndhevelsessektoren. EUs agentur for grunnleggende rettigheter

³ Se for eksempel direktivets foralepunkt 7 og 15.

⁴ C-210/16.

(FRA) har kommet med en slik tolkning.⁵ Vi viser også til Artikkel 29 gruppens uttalelse 01/2014 om nødvendighets- og proporsjonalitetsprinsippet i rettshåndhevelsessektoren.

Vi mener det bør utformes en egen bestemmelse i politiregisterloven som gjennomfører LED artikkel 4 om prinsipper. En egen bestemmelse om prinsipper vil i større grad bidra til harmonisering og brukervennlighet. Vi er også usikre på hvorfor ikke alle personvernprinsippene er gjennomført i politiregisterloven. Vi trekker særlig frem rettferdighetsprinsippet, som er et av de mest sentrale personvernprinsippene.

Bruk av ny teknologi og metoder

Vi mener personvernkommisjonen bør se nærmere på politiets adgang til å ta i bruk ny teknologi som "big data", kunstig intelligens, automatiserte avgjørelser og profilering. Politiets virksomhet er i aller høyeste grad informasjonsstyrt. Det er derfor et stort potensiale for politiet i å ta i bruk ny teknologi, for eksempel for å oppnå effektivisering og mer presis informasjonsbehandling. Dette gjelder i hele politiets arbeidskjede fra forebyggende arbeid til bruk av politiets beredskapsressurser i tidskritiske sammenhenger, og for etatens virksomhetsstyring. Samtidig kan bruk av slik teknologi innebære betydelige inngrep i den enkeltes rett til personopplysningsvern. Vi mener personvernkommisjonens arbeid på dette området kan gi et viktig bidrag for å finne det riktige balansepunktet mellom de grunnleggende interesser.

Om automatiserte avgjørelser og profilering

LED artikkel 11 inneholder et forbud mot avgjørelser som utelukkende er basert på automatisert behandling, herunder profilering, med mindre det gjøres unntak i nasjonal rett.

Direktivbestemmelsen er gjennomført i både Danmark og Sverige, men ikke i Norge.⁶ I lovforarbeidene til politiregisterloven er det slått fast at det ikke er nødvendig å gjennomføre LED artikkel 11. Begrunnelsen er at "... det i Norge ikke er ordninger der individuelle avgjørelser som er av betydning for den det gjelder utelukkende er basert på automatisk behandling."⁷ Vi setter spørsmålsteget ved om dette er fyllestgjørende, og trekker særlig frem Artikkel 29 gruppens tolkning av direktivbestemmelsen.⁸

Vi mener LED artikkel 11 bør gjennomføres i norsk rett. I hvilken grad politiet bør kunne nyttiggjøre seg av slik teknologi bør drøftes av personvernkommisjonen.

Om bruk av informasjon som er offentliggjort

LED artikkel 10 bokstav gir et rettslig grunnlag for behandling av særlige kategorier av opplysninger. Det følger av bestemmelsen at behandlingen må være strengt nødvendig og det må gis tilstrekkelige garantier. I bestemmelsens bokstav c åpnes det opp for at slike opplysninger kan behandles når behandlingen gjelder opplysninger som det er åpenbart at den registrerte har offentliggjort.

⁵ Se "Handbook on European data protection law – 2018 edition" side punkt 8.2.1.

⁶ Se lov om retshåndhevelse myndigheters behandling af personoplysninger § 11, og brottsdatalog 19 §.

⁷ Se Prop.99 L (2016-2017) side 13.

⁸ Se WP 258 side 11 til 15, herunder eksemplene som gis på side 12.

Artikkel 10 bokstav c er gjennomført i andre medlemsland, men ikke i Norge.⁹ Begrunnelsen for dette følger blant annet av lovforarbeidene til politiregisterloven. Der opplyses det at dette ikke bør være et "selvstendig grunnlag for politiets behandling når vilkårene for formålsbestemthet og nødvendighet ikke er oppfylt."¹⁰ Vi er noe usikre på hva som ligger i denne begrunnelsen. LED artikkel 10 inneholder krav om strengt nødvendig, og bestemmelsen må ses i sammenheng med øvrige krav i LED, herunder prinsippet om formålsbestemthet i artikkel 4.¹¹ Artikkel 29 gruppen har for øvrig foretatt en tolkning av både krav til strengt nødvendig, tilstrekkelig garantier og grunnlaget for behandling i bokstav c.¹²

I lys av den teknologiske utviklingen og digitaliseringen er dette et praktisk viktig grunnlag. Vi mener derfor at LED artikkel 10 bokstav c bør gjennomføres i norsk rett, og at personvernkommisjonen bør drøfte grensene for politiets adgang til å bruke opplysninger som den registrerte selv har offentliggjort.

Samhandling med andre kontrollmyndigheter

Mer og mer av rettshåndhevingen i samfunnet blir lagt til offentlig forvaltning. Oppgaver som tradisjonelt har vært hos politi, påtalemyndighet og domstoler hører nå inn under ulike forvaltningsorgan.¹³

Vi mener denne utviklingen tilsier at personvernkommisjonen bør drøfte rammene for lovlig utveksling av personopplysninger mellom politiet og slike offentlige kontrollmyndigheter. Det er viktig at det gjøres grundige vurderinger av de krav som følger av både LED og personvernforordningen. Vi peker spesielt på lovlighets-, nødvendighets- og proporsjonalitetskravet.¹⁴ EPDS¹⁵ har for øvrig utarbeidet en nyttig veileder om nødvendighetskravet.¹⁶

Vi mener i tillegg at det er forhold ved gjennomføringen av LED i norsk rett som bør trekkes inn i et slikt arbeid. LED gjelder for "kompetente myndigheters" behandling av personopplysninger for formålene som følger av artikkel 1 nr. 1, se artikkel 2 nr. 1. Begrepet kompetente myndigheter defineres i LED artikkel 3 nr. 7.¹⁷ Selv om politiet er det sentrale eksempelet på en slik myndighet, kan også andre myndigheter være omfattet av definisjonen. Politiregisterloven gjelder imidlertid kun for politiets og påtalemyndighetens behandling av personopplysninger, jf. lovens § 3.

⁹ For eksempel i Danmark, se lov om retshåndhævende myndigheders behandling af personoplysninger § 10.

¹⁰ Se Prop.99 L (2016-2017) side 15.

¹¹ I samme retning se Artikkel 29 gruppens uttalelse 6/2014 punkt III.2.3 om forholdet mellom rettslig grunnlag og personvernprinsipper.

¹² Se Artikkel 29 gruppens uttalelse WP 258 side 7 til 8 og 10 til 11.

¹³ Meld. St. 11 Personvern – utsikter og utfordringer punkt 4.6.

¹⁴ Prinsippene er nærmere beskrevet i Datatilsynets høringsuttalelse av 16.10.2017 om utkast til ny personopplysningslov.

¹⁵ European Data Protection Supervisor, som er EUs datatilsynsombudsmann.

¹⁶ Se følgende nettside: [https://edps.europa.eu/sites/edp/files/publication/17-06-](https://edps.europa.eu/sites/edp/files/publication/17-06-01_necessity_toolkit_final_en_0.pdf)

[01_necessity_toolkit_final_en_0.pdf](https://edps.europa.eu/sites/edp/files/publication/17-06-01_necessity_toolkit_final_en_0.pdf)

¹⁷ Se også fortalens punkt 11.

LED har altså et potensielt videre virkeområde enn det har fått i norsk rett.¹⁸ Konsekvensen er at personvernforordningen gjelder for offentlige myndighetsorganer som kunne vært omfattet av LED. Selv om mye av regelverket er likt er det også klare forskjeller mellom LED og personvernforordningen. Poenget vårt er at det kan være grunn til å foreta en vurdering av om flere offentlige myndigheter bør være omfattet av LED sitt saklige virkeområde. Vi mener ikke med dette at politiregisterlovens saklige virkeområde bør utvides, men om andre kontrollmyndigheter med tilhørende sektorlovgivning også bør være omfattet av direktivet.

Sammensetning av personvernkommisjonen

Personvernkommisjonen bør ha en bred sammensetning med blant annet teknologer, samfunnsvitere og jurister. Vi mener det også er viktig at flere av representantene kommer fra justissektoren, herunder personer med kunnskap og kompetanse om hvordan politiet behandler og bruker opplysninger, herunder i politiregistre og andre systemer.

Med hilsen



Sveinung Sponheim
Visepolitimester



Bård Soløy Ødegaard
Seniorrådgiver

¹⁸ I Sverige er LED gitt et vidt virkeområde, se brottsdatalag 2 §.

