POLITIET
KRIPOS

Politidirektoratet
politidirektoratet@politiet.no

NCIS Norway

Deres referanse:	Vår referanse:	Sted, dato
	2018/00727	Oslo, 13.08.2018

PERSONVERNKOMMISJONEN – INNSPILL TIL MANDAT

Det vises til Politidirektoratets e-post av 23. juli 2018 vedrørende innspill til mandat til Personvernkommisjonen 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 personvernkommisjonen 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

Post: Pb. 2094 Vika, 0125 Oslo
Besøk: Brynsalléen 6, 0667 Oslo
www.politi.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 sikkerhetselement 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 ikrafttredelsen 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 ikrafttredelsen 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 ikrafttredelsen 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 føretil 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 høringssvar 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 avgjørelser[5]. 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[6] 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

[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.

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 innhentingen 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
Ivaretakelse 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