POLITIET
KRIPOS

Politidirektoratet
Postboks 2090 Vika
0125 Oslo

Kripos

Deres referanse:	Vår referanse:	Dato:
	22/223377 - 63	13.01.2023

Høringssvar - NOU 2022:11 Ditt personvern - vårt felles ansvar - Personvernkommisjonens rapport

Det vises til brev fra Kommunal- og distriktsdepartementet av 11. november 2022. Videre vises det til brev fra Politidirektoratet av 24. november 2022, hvor frist for eventuelle merknader til utredningen er satt til 13. januar d.å.

Kommisjonens utredning løfter mange relevante utviklingstrekk og problemstillinger. Kripos oppfatter det overordnede budskapet som at retten til personvern, som en grunnleggende menneskerettighet, må være på dagsorden - også i de mange og omfattende digitaliseringsprosessene som skjer i Norge. Rapporten får også frem det samfunnsmessige behovet for godt personvern.

Kripos er behandlingsansvarlig for 18 av 20 sentrale politiregistre, og har også et nasjonalt veiledningsansvar for personvern i politiet. Som særorgan, med spesialiserte bistandsmiljøer innenfor blant annet digital og teknologidrevet kriminalitet, møter Kripos daglig avveininger mellom kriminalitetsbekjempelse og personvern. Kripos har på forespørsel levert to notater til utvalget underveis i utredningen og har hatt dialog med utvalgets sekretariat. Som det fremgår av utredningen har også to representanter fra Kripos gjennomført møte med deler av utvalget.

Utredningen omtaler utviklingen innenfor mange samfunnsområder, og gir en rekke anbefalinger. Kripos har begrenset sine merknader til det som er mest relevant for Kripos' ansvar, oppgaver og kompetanse. Som politiorgan vil NOUens kapittel 7 om personvern i justissektoren gis mest omtale. Som en del av offentlig forvaltning, med samarbeidsflater mot en rekke andre aktører, vil vi også knytte noen merknader til kapittel 6 om personvern i den digitale forvaltningen. Merknadene følger rapportens inndeling og nummerering.

Til kapittel 6 – personvern i den digitale forvaltningen

6.1.2 Viktigheten av tillit til offentlig forvaltning

Kripos er enig i at tillit til offentlige myndigheter er en forutsetning for et velfungerende demokrati. For politiets del kan tillit fra publikum også være avgjørende for oppgaveløsningen,

Post: Postboks 2094 Vika, 0125 Oslo
Tlf: (+47) 23 20 80 00
Org. nr: 974760827
E-post: kripos@politiet.no
www.politiet.no

herunder for tilgang til informasjon som politiet er avhengig av. Tillit til at personopplysninger behandles forsvarlig av offentlige myndigheter er en vesentlig del av dette, noe som fordrer størst mulig grad av åpenhet og informasjon.

Kripos vil imidlertid fremheve at også effektivitet i oppgaveløsningen er sentralt for å sikre og opprettholde slik tillit. Kommisjonen nevner blant annet regler om taushetsplikt, behandlingsgrunnlag og formålsbegrensning som sentrale for å verne innbyggernes integritet og autonomi, og at slik regulering bidrar til å sikre innbyggernes tillit til offentlig forvaltning.

Det er opplagt et behov for denne type regler også internt mellom forvaltningsorganer, men i dag eksisterer det en rekke kompliserte regelsett i ulike sektorer - hvor det i praksis kan være uklart hvor langt disse rekker. Det brukes mye ressurser på tolkning og veiledning internt i hver sektor, og det oppstår særlige problemstillinger i tverrsektorielt samarbeid. Justis- og beredskapsdepartementet har fått utarbeidet et utkast til veileder om taushetsplikt, opplysningsplikt og opplysningsrett i forvaltningen.[1] Slik Kripos ser det viser både selve utkastet til veileder, og i enda større grad de publiserte høringssvarene til utkastet, at gjeldende regelverk er komplisert og at denne kompleksiteten i seg selv kan være til hinder for effektiv oppgaveløsning. For Kripos fremstår det sentralt at hensynet til et praktikabelt og sammenhengende lovverk blir vektlagt i større grad når det blir foreslått regler om taushetsplikt, behandlingsgrunnlag og formålsbegrensinger.

Kommisjonen viser videre til at det er viktig for tilliten at viderebehandling av personopplysninger skjer i tråd med innbyggernes forventninger, og at det kan oppfattes som et tillitsbrudd om opplysninger som er samlet inn for et konkret formål brukes til nye formål i en annen kontekst. Kripos er enig i at tillitt og forventninger henger nøye sammen. Samtidig vil innbyggernes forventninger kunne variere, og likeså styrken i de hensyn som eventuelt tilsier videre bruk av opplysninger til andre formål enn innsamlingsformålet. Blant annet kan kvalitets- og effektivitetshensyn tale for gjenbruk. For Kripos' synes dette i mange tilfeller vel så mye å være et spørsmål om informasjon og kommunikasjon. Om en innbygger vil oppfatte bruk til andre formål som et tillitsbrudd, dersom vedkommende var godt opplyst om årsaken til og styrken i de hensyn som begrunner slik bruk, fremstår for oss som usikkert. Dette er avveininger lovgivningsprosessen etter vårt syn skal være og er godt egnet til å avklare og ivareta.

6.4 Personvernutfordringer knyttet til deling og viderebehandling av personopplysninger i offentlig forvaltning

Kommisjonen fremmer her følgende anbefalinger som Kripos har merknader til:

Personvernkommisjonen anbefaler at ansvarsfordelingen i større grad lov- eller forskriftsfestes der deling av personopplysninger inngår som del av et større samarbeid mellom forvaltningsorganer og hvor uklarhet kan medføre alvorlige personvernkonsekvenser.

Kripos' utgangspunktet er at behandlingsansvaret går over fra organet som utleverer personopplysninger til organet som mottar personopplysningene, i det opplysningene er

[1] https://www.regjeringen.no/no/dokumenter/horing-utkast-til-veileder-om-taushetsplikt-opplysningsplikt-og-opplysningsrett-i-forvaltningen/id2834815/

kommet frem til mottaker. Etter mottak vil det også være mottakerorganets regler om for eksempel taushetsplikt som kommer til anvendelse.[2]

Utgangspunktet bør likevel ikke strekkes for langt. Som personvernkommisjonen peker på, kan det oppstå uklarheter i mer etablerte samarbeid mellom forvaltningsorganer, særlig hvor det benyttes felles IT-systemer. Her ser vi i dag ulike og, i en del tilfeller, svært kompliserte ansvarsmodeller – uttrykt i databehandleravtaler, samarbeidsavtaler og lignende. I slike situasjoner er vi enige med kommisjonen i at behandlingsansvaret bør vurderes fastsatt i forskrift. Det kan i slike tilfeller være fordelaktig om ett organ alene gis ansvaret for informasjonssikkerheten i systemet, mens øvrige deltakende organer gis ansvar for kvaliteten og lovligheten til de opplysninger organene tilfører systemet.

Vi er imidlertid skeptiske til stor grad av lovregulering av behandlingsansvar, siden samarbeid mellom forvaltningsorganer og tilhørende IT-systemer gjerne er i hyppig utvikling. Dersom ansvarsforholdene "sementeres" gjennom formell lov, kan det oppstå et økende misforhold mellom det formelle ansvaret og de faktiske arbeidsprosesser og understøttende systemer.

Personvernkommisjonen mener offentlige virksomheter må gjøre grundige vurderinger av om de skal benytte sosiale medier for å gi informasjon og kommunisere med innbyggerne. Sosiale medier bør ikke brukes i konkret enkeltsaksbehandling.

Kripos støtter kommisjonens anbefalinger på dette punktet. Som et ledd i Kripos' arbeid med politiets åpne tilstedeværelse på internett, har vi fått utviklet tjenesten "Sikker chat for nettpatruljene". Formålet med tjenesten er blant annet å kunne flytte kontakt med politiet på sosiale medier over på en kanal som bedre sikrer informasjonssikkerhet og notoriet. Sikker chat erstatter ikke andre kommunikasjonskanaler med politiet, men fungerer som et supplement – særlig for yngre målgrupper.

Personvernkommisjonen mener det er viktig at det gjøres både personvern- og datastrategiske vurderinger når det offentlige benytter tjenester fra store teknologiselskaper. Fordi spørsmålene ofte er likelydende, bør forvaltningen samarbeide på tvers av sektorer og nivåer for å sikre høy faglig kvalitet og god bruk av ressurser.

Kripos støtter denne anbefalingen. Slik Kripos ser det kan SKATE[3], eventuelt gjennom arbeid i undergrupper, være et godt egnet fora for slikt samarbeid.

Til kapittel 7 – Personvern i justissektoren

7.1.2 Personvern i justissektoren – en rettssikkerhetsgaranti

I dette punktet fremhever Personvernkommisjonen merknadene til politiregisterloven § 1 om lovens formål. Kommisjonen referer til følgende punkt i Ot. Prp.nr. 108 (2008-2009):

Formålet vil være et moment ved tolkingen av de andre bestemmelsene i loven, særlig der politi og påtalemyndighet er tillagt et visst skjønn. I de tilfellene der hensynet til personvern og hensynet til kriminalitetsbekjempelsen ikke kan forenes, er utgangspunktet at hensynet til

[2] Unntak der mottaker pålegges ytterligere taushetsplikt, jf. for eksempel politiregisterloven § 35.
[3] https://www.digdir.no/skate/skate/1259

personvernet må vike. Ved denne avveiningen skal det imidlertid alltid foretas en forholdsmessighetsvurdering.

Kommisjonen viser til at den ikke er enig i dette, og at "når interesser står mot hverandre, kan ikke utgangspunktet være at personvernet alltid må vike".

Det er viktig å forstå konteksten for utsagnet i forarbeidene. Slik Kripos vurderer denne er det ikke grunnlag for å tolke forarbeidene som et generelt utsagn om at personvern alltid må vike for hensynet til kriminalitetsbekjempelse hvor disse hensynene er i konflikt. Politiregisterloven som sådan skal både bidra til å fremme kriminalitetsbekjempelsen og personvernet. Hvor ordlyden i reglene er klare, er også avveiningen mellom ulike hensyn i stor grad gitt.

7.1.3 Viktigheten av tillit til justissektoren

Kripos tiltrer Personvernkommisjonens utgangspunkt.

7.3.4 Politiske føringer – utvidelse av politimyndighetenes inngrepsmuligheter

Personvernkommisjonen viser til at Rådet i EU har lagt frem forslag til endringer i Europol Regulation, som i større grad åpner opp for behandling av store datasett hvor de gjeldende krav til kategorisering mykes opp. Forslaget er kommet i kjølvannet av at European Data Protection Supervisor (EDPS) har pekt på avvik i Europols behandling av personopplysninger på dette området. Kommisjonen viser til at forslaget har blitt kritisert av EDPS. Kommisjonen fremmer følgende anbefaling:

Personvernkommisjonen mener funnene EDPS har avdekket om at EUROPOL mottar store mengder personopplysninger fra politiet i medlemsland må følges opp av norske myndigheter for å sikre at personvernet til norske innbyggere blir ivaretatt når politiet overfører opplysninger til EUROPOL. Kommisjonen antar at tilsvarende problemstillinger kan foreligge i andre sammenhenger hvor informasjon utveksles mellom politimyndigheter, for eksempel mellom Norge og INTERPOL, og at dette også må følges opp.

Kripos har nylig fastsatt retningslinjer for utlevering av opplysninger til utlandet i internasjonalt politisamarbeid. Retningslinjene utdyper og konkretiserer forpliktelsene i politiregisterloven § 22 og politiregisterforskriften kapittel 70. Utlevering skjer i enkelttilfeller og vurderes konkret. Kripos vil vurdere å oppdatere retningslinjen med særlige krav til eventuell utlevering av store datasett til utlandet.

7.4.1 Personvern i lovarbeid

Kripos vil, som kommisjonen, understreke betydningen av at personvernkonsekvenser grundig belyses og utredes som del av lovforarbeider. Innenfor justissektoren vil mange lover og forskrifter påvirke og berøre personvernet. Dette innebærer ikke nødvendigvis en konflikt mellom regel og personvern. Som kommisjonen selv uttaler i punkt 7.1.2; "*I flere sammenhenger vil en tilstrekkelig kriminalitetsbekjempelse utvilsomt være en forutsetning for godt personvern,…".*

Under dette punkt fremmer kommisjonen påstand - om at "*….vurderinger av personvernkonsekvenser kan være begrensede og mangelfulle i forbindelse med nye lov- og forskriftsforslag.*" og at " *Eksemplene over illustrerer at det er tydelige mangler ved*

vurderinger av personvernkonsekvenser i lov- og forskriftsarbeider." Særlig sistnevnte påstand fremstår for Kripos som overdreven hensett til de grunnlag det vises til. Kommisjonen viser blant annet til flere eksempler fra høringsprosesser hvor Datatilsynet har fremmet innsigelser uten å få fult ut gehør for disse. For Kripos synes eksemplene i vel så stor grad å underbygge at lovprosessene er grundige. At man ikke alltid får gehør for synspunkter utgjør i seg selv ikke et godt grunnlag for å påstå at prosessen ikke fungerer og har mangler ved seg.

7.4.2.1 Implementering av politidirektivet i politiregisterloven

Kommisjonen anser at politiregisterloven ikke oppstiller tilstrekkelige konkrete krav og føringer for behandling av personopplysninger, og anbefaler at loven forenkles og forbedres.

Slik Kripos vurderer det oppstiller politiregisterloven viktige prinsipper og hovedregler, som blir detaljert i betydelig grad gjennom politiregisterforskriften. Politiregisterforskriften er omfattende, og gir for mange viktige behandlinger svært konkrete krav og føringer. Samtidig er deler av forskriften preget av mange henvisninger til andre bestemmelser og unntak fra hovedregler. Dette gjelder blant annet reglene om vandelskontroll. Reglene skal ivareta flere kryssende hensyn og de endres relativt hyppig. Dette gjør at praktisk viktig regelverk om for eksempel hva som skal fremkomme på politiattest, blir vanskelig tilgjengelig.[4]

Slik Kripos ser det er ikke kommisjonens forventninger om både konkrete krav/føringer på den ene siden og brukernes erfarte behov for forenklinger i regelverket lett forenelig. Det er uansett et klart behov for evaluering av politiregisterlov og forskrift, og dagens detaljeringsgrad bør inngå i en slik evaluering.

Kommisjonen fremmer følgende anbefaling:

Personvernkommisjonen mener Justis- og beredskapsdepartementet må vurdere om alle bestemmelsene i politidirektivet skal implementeres i politiregisterloven. En harmonisering av loven med direktivet vil gi klarere retningslinjer for personvernvurderinger og gjøre det enklere for tjenestepersoner å anvende loven.

Kripos støtter en ytterligere harmonisering mellom politidirektivet (direktiv 2016/680EU) og politiregisterloven. Utover de bestemmelser i direktivet som kommisjonen viser til, vil Kripos fremheve artikkel 11 om profilering og automatiserte avgjørelser. Som kommisjonens rapport viser er dette spørsmål med stadig økende aktualitet også i norsk rett. Kripos følger imidlertid ikke kommisjonen i at en ytterligere harmonisering mellom politiregisterloven og politidirektivet nødvendigvis vil gjøre det enklere for tjenestepersoner å anvende politiregisterloven. Direktivet er i stor grad prinsippbasert, og systematikken er i hovedsak lik som personvernforordningen – som kommisjonen i sin rapport beskriver som komplisert.

7.4.2.2 Bruk av åpne kilder

Kommisjonen fremmer følgende anbefaling:

Personvernkommisjonen mener bruk av åpne kilder på internett kan skape særskilte personvernutfordringer. Kommisjonen er blant annet bekymret for hvilke nedkjølingseffekter

[4] Se blant annet vårt høringssvar til forslag til endringer i konfliktrådsloven, straffeloven mv. datert 19. desember 2022.

som kan oppstå som følge av justissektorens bruk av åpne kilder på nett, og dette perspektivet må vektlegges ved utarbeidelse av interne instrukser og lignende.

Personvernkommisjonen nevner Kripos' veileder om politiets bruk av åpne kilder på internett fra 2018. Veilederen har blitt oppdatert i 2022, og beskrivelsen av de rettslige rammene har blitt utvidet.

Kripos deler ikke kommisjonens synspunkter om bruk av åpne kilder. Så lenge politiregisterlovens ordinære regler, blant annet om nødvendighet, formålsbestemthet og forholdsmessighet, blir overholdt, ser ikke Kripos at bruk av opplysninger fra åpne kilder på internett byr på særlige utfordringer i forhold til andre kilder til informasjon som politiet har tilgjengelig. Opplysninger som brukes i straffesak må nødvendigvis settes i sin rette kontekst, på lik linje med alle andre opplysninger i saken. Det som *kan* by på utfordringer er innhenting og lagring av store datasett generelt, hvor det bare er en mindre del av opplysningene som har betydning for politiets oppgaveløsning.

Kommisjonen fremhever en mulig nedkjølingseffekt på ytringsfriheten. En slik effekt kan være bekymringsverdig. Slik Kripos' ser det hadde det imidlertid vært fordelaktig med mer kunnskap om både arten og styrken av en slik effekt, før den eventuelt tillegges slik vekt som kommisjonen synes å gjøre.

7.4.2.4 Formålsutglidning i forbindelse med politiets myndighetsutøvelse

Personvernkommisjonen mener ledelsen i politiet må ha høy bevissthet om faren for formålsutglidning, og at risikoen for slik utglidning må reduseres gjennom etablering av organisatoriske og tekniske tiltak. Et viktig tiltak i denne sammenheng er å bygge en god personvernkultur. Dette er et lederansvar.

Det er lett å støtte kommisjonen i at engasjement og fokus fra ledelsen - her som på andre sentrale områder i en organisasjon – vil være viktig for en god kultur. Personvern i politiet har gått igjennom en betydelig utvikling siden ikrafttredelsen av politiregisterloven og politiregisterforskriften i 2013, og det etterfølgende SPOR-programmet. Utviklingen er ikke avsluttet, og det er flere initiativ både i regi av Politidirektoratet og Kripos for å styrke personvernet i politiet ytterligere.

Kripos har gode erfaringer med den årlige ledelsens gjennomgang. Ved Kripos rapporterer hver avdeling på rutiner, avvik og vesentlige risikoer, som sammenstilles av personvernseksjonen. Det skriftlige materialet gjennomgås av sjef Kripos, og det avholdes møter hvor avdelingene rapporterer. Prosessen bidrar til kontinuerlig bevissthet om personvern hos ledelsen på alle nivåer.

7.4.2.5 Deling av opplysninger mellom politiet og andre myndigheter

Kripos er enig i kommisjonens vurderinger på dette punktet, og viser til våre merknader til punkt 6.1.2 over.

7.4.3 Åpenhet om politiets metodebruk

Kommisjonen fremmer følgende anbefalinger:

Personvernkommisjonen anbefaler at det nedsettes et utvalg for å utrede metodebruken i justissektoren. Utvalget bør særlig vurdere personvernkonsekvenser av politiets metoder, særlig sett opp mot formålsprinsippet og proporsjonalitetsprinsippet. Dette arbeidet forutsetter at utvalget har tilgang på nødvendig informasjon om bruken av inngripende metoder og skjulte tvangsmidler. Dette er viktig både som et tillitsbevarende tiltak, og for å reise en åpen og demokratisk debatt om hvor grensen mellom personvern og kriminalitetsbekjempelse og forebygging bør gå.

Metodebruk i justissektoren er et omfattende tema. Som beskrevet tidligere i kommisjonens utredning er det et skille mellom innhenting av opplysninger gjennom tvangsmidler, som reguleres av straffeprosessloven, og den etterfølgende behandlingen som reguleres av politiregisterloven med forskrift. Dette skillet er ikke gjort fullt ut for opplysninger fra skjulte tvangsmidler som for eksempel kommunikasjonskontroll, hvor straffeprosessloven regulerer etterfølgende behandling av advokatsamtaler og nærståendesamtaler i kapittel 16a. Her foreligger det også mye rettspraksis, hvor kjennskap til denne er helt nødvendig for å fastlegge reglenes nærmere innhold. Kripos har i tidligere høringsprosess[5] foreslått en nærmere utredning av handlingsrommet for tilpasset *innhenting* av opplysninger ved bruk av kommunikasjonskontroll mv.

Den teknologiske utviklingen vil kontinuerlig utfordre både lovgivning, praksis og kontrollkjede. Dette kan tilsi et behov for å vurdere også deler av hjemmelsgrunnlaget for metodebruken i justissektoren. Det må samtidig bemerkes at den regelutvikling som har funnet sted innenfor politiets metodebruk de senere år, herunder endringer i straffeprosessloven, har kommet som resultat av omfattende lovarbeid inkludert grundige utredninger og høringsprosesser. Det er etter vår vurdering intet i disse prosessene som i seg selv skulle tilsi behov for et nytt metodeutvalg.

Kommisjonen uttaler at det har vært "…utfordrende å få innsikt i metodebruk og verktøy som er i bruk eller som vurderes tatt i bruk". Om dette skyldes tilbakeholdenhet hos politiet, manglende kapasitet hos kommisjonen, eller lovbestemt taushetsplikt, jf. punkt 7.4.5.1 nedenfor, synes uklart. Kripos er uansett enig med i kommisjonen i at enhver utredning forutsetter tilgang til nødvendig informasjon, herunder tilgang til informasjon omfattet av taushetsplikt i den grad slike opplysninger er nødvendig for de vurderinger som skal foretas.

7.4.4 Effektiv domstolskontroll

Kommisjonen viser til at det i 2016 ble fremmet en proposisjon om endringer i straffeprosessloven, at forslaget innebar å gi en utvidet adgang til å benytte skjulte tvangsmidler, og at dersom forslaget hadde blitt vedtatt hadde "domstolskontrollen blitt redusert til en vurdering av om tiltakene var forholdsmessige og saklig begrunnet". Kripos leser ikke forarbeidene slik, og kan heller ikke finne støtte for utvalgets uttalelser i referansene som oppgis til Prp. 68 L (2015-2016), fotnote 168 og 169.

[5] Blant annet i høringssvar til endringer i politiregisterloven datert 26. august 2020

Kommisjonen fremmer følgende anbefalinger:

Personvernkommisjonen mener det bør vurderes om dagens domstolskontroll av politiets tiltak bør utvides til å omfatte flere tiltak enn i dag. Kommisjonen understreker videre viktigheten av at bestemmelser som hjemler forskjellige tvangsmidler formuleres slik at effektiv og reell domstolskontroll blir mulig.

Kripos kan vanskelig se at det som trekkes frem av kommisjonen under dette punkt gir grunnlag for en godt begrunnet slutning om at *utvidet domstolskontroll til å omfatte flere tiltak* bør vurderes. Det betyr ikke at dagens domstolskontroll ikke kan forbedres. Kripos erfarer - særlig innen enkelte former for teknologisk tvangsmiddelbruk – at de vurderinger domstolen skal foreta fordrer høy kompetanse, herunder teknologisk kompetanse. Dette reiser spørsmål om blant annet behov for spesialisering – også i domstolen. Kripos viser for øvrig til våre merknader under punkt 7.3.4 ovenfor.

7.4.5.1 Kommersielle analyseverktøy for bruk i justissektoren

Kommisjonen fremmer her følgende anbefaling:

Personvernkommisjonen mener det er avgjørende med åpenhet og muligheter for kontroll ved anskaffelser i justissektoren. Ved anskaffelse av potensielt inngripende verktøy må personvernvurderinger være en sentral del av beslutningsgrunnlaget.

Kripos er enig i at den klare hovedregel ved anskaffelser bør være åpenhet. Samtidig har politiet i en del sammenhenger behov for å kunne beskytte sine metoder, og slik informasjon kan etter omstendighetene være omfattet av taushetsplikt, jf. blant annet politiregisterloven § 23 annet ledd. Det faktum at politiet har anskaffet visse typer spesialprogramvare kan i seg selv avsløre sensitive metoder.

Kontrolletater som Datatilsynet, Sivilombudet, Riksrevisjonen, EOS-utvalget og Kontrollutvalget for kommunikasjonskontroll kan uten hinder av taushetsplikt innhente informasjon om systemanskaffelser innenfor sitt kontrollområde.

Kripos har utarbeidet en mal for personvernkonsekvensvurderinger etter politiregisterforskriften, og en veileder for denne. Personvernkonsekvensvurderinger gjøres blant annet ved anskaffelser som kan ha vesentlige personvernkonsekvenser, ved nyutvikling, og hvor eksisterende programvare tas i bruk til nye formål. Gode personvernkonsekvens-vurderinger krever ofte både teknisk fagkunnskap, kunnskap om hvordan systemet vil bli brukt (brukerperspektiv) og personvernkompetanse.

7.4.5.2 Utfordringer ved bruk av maskinlæringsmodeller i justissektoren

Kripos er enig i at ansvarlig bruk av maskinlæringssystemer fordrer gode forhåndsvurderinger og at det foreligger grundig dokumentasjon av systemet. Slike systemer kan ha feilkilder, og det er svært viktig å ikke ta dem i bruk til formål de ikke er egnet til.

Personvernkommisjonen beskriver i dette punktet bruk av maskinlæringssystemer til profilering og prediksjon, og skriver blant annet "[n]år maskinlæringssystemet skal trenes, legger utvikleren som regel inn all informasjon man vurderer som relevant for systemets oppgaver. Det kan inkludere inntekt, hvor man bor, om man har kriminelle foreldre og en lang

rekke andre faktorer som kan vurderes som relevante". Denne beskrivelsen kan sikkert være riktig, men Kripos finner grunn til å bemerke at eventuell bruk av maskinlæring på en slik måte ligger langt utenfor hva som gjøres i norsk politi gjør i dag, og hva politiregisterloven vil tillate.

Det mest relevante eksempelet for politiet i dag er programvare for ansiktsgjenkjenning. Forsvarlig bruk av ansiktsgjenkjenningsteknologi er viktig for politiets arbeid i dag, og forventes like viktig i tiden fremover. Det er slik Kripos ser det viktig å differensiere mellom ulike former for bruk av ansiktsgjenkjenning, og til hvilke formål teknologien brukes. For eksempel vil bruk til sortering av store bildematerialer fra konkrete beslag i straffesaker kunne bidra til sakens oppklaring uten særlig personvernkonsekvens. Motsetningsvis vil bruk av teknologien i sanntid, på offentlig sted, innebære en vesentlig personvernkonsekvens – som også kommisjonen peker på.

Kommisjonen fremmer her følgende anbefaling:

Personvernkommisjonen mener det bør tas spesielt hensyn til etterprøvbarhet og ivaretakelse av den enkeltes rettigheter ved bruk av maskinlæringssystemer i justissektoren. For at slike metoder skal kunne tas i bruk i Norge, må de også være forklarbare for den som anvender teknologien, og risikovurderinger og pålagt teknisk dokumentasjon må foreligge i tråd med forslaget om forordning for kunstig intelligens.

Forslaget til ny EU-forordning om kunstig intelligens (AI-forordningen)[6] har som kommisjonen viser til regler om blant annet etterprøvbarhet, risikovurderinger og dokumentasjon. Det er verdt å merke seg at det er gjort unntak fra forordningens åpenhetsregler for systemer som benyttes for å avdekke, forebygge, etterforske eller iretteføre straffbare forhold, jf. artikkel 52.

7.4.5.3 Utfordringer ved bruk av store datamengder

Kommisjonen fremmer her følgende anbefalinger:

Personvernkommisjonen anbefaler et generelt forbud mot bruk av ansiktsgjenkjenning og annen biometrisk fjernidentifikasjon i offentlige rom. Et slikt forbud vil åpenbart begrense mulighetene for oppklaring av enkelte former for kriminalitet, men etter kommisjonens syn er teknologien såpass inngripende at det vanskelig kan forenes med grunnleggende rettigheter og samfunnsverdier.

Forslaget til AI-forordning har regler om biometrisk fjernidentifikasjon i offentlige rom, og oppstiller i utgangspunktet et forbud mot dette. Forslagsteksten, slik den foreligger nå, åpner imidlertid for snevre unntak i nasjonal lovgivning, jf. artikkel 5. Kripos kan ikke se at norsk myndigheter bør unngå å bruke dette handlingsrom for bruk av ansiktsgjenkjenning i forhold til den alvorligste kriminalitet rettet mot liv og helse.

For Kripos' fremstår det uklart om Personvernkommisjonen bifaller forslaget til AI-forordning på dette punktet, eller foreslår nasjonal lovgivning på siden av eller i stedet for forordningens reguleringer av biometrisk fjernidentifikasjon. Dersom forordningen anses som EØS-relevant, og det tas sikte på totalharmonisering, er det uklart hvilket nasjonalt handlingsrom som

[6] Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence, 21. april 2021.

eksisterer. Kripos anbefaler følgelig at departementet følger utviklingen på dette området i EU nøye, fremfor å fremme nasjonale regelforslag på nåværende tidspunkt.

7.4.6 Personvernkompetanse

Kommisjonen fremmer her følgende anbefalinger, som Kripos omtaler samlet:

Personvernkommisjonen kan ikke se at politiet i tilstrekkelig grad har vektlagt å øke medarbeidernes bevissthet rundt personvern. Personvernkompetanse og -kultur må forankres i ledelsen i politiet. Det må også vies ressurser til at personvernombud kan legge til rette for kompetanseheving i organisasjonen.

Personvernkommisjonen mener tjenestepersoner i politiet bør ha grundigere opplæring i personvern enn det som i dag er tilfellet. Behovet er spesielt stort i forbindelse med bruk av IKT-systemer i det daglige politiarbeidet, ved personvern og menneskerettighetsvurderinger ved innhenting og utlevering av personopplysninger, og ved samarbeid med andre offentlige eller private virksomheter.

Kripos vil bemerke at grunnopplæring i personvern er obligatorisk for alle nyansatte i politiet, gjennom e-læringskurs. Det er et utvidet kurs for påtroppende ledere. Personvernreglene er også inntatt i obligatoriske kurs for spesielle politisystemer som Indicia, hvor kravene til etterretningsregisteret i politiregisterforskriften kapittel 47 både er omtalt og hensyntatt i den praktiske opplæringen. Kripos har også utarbeidet et større antall veiledninger og tiltakskort for etaten, særlig når det kommer til utlevering av opplysninger – som er et meget praktisk spørsmål når politiet samarbeider med andre offentlige eller private virksomheter, sml. merknadene til punkt 6.2.1 ovenfor.

Som dette, samt våre merknader til punkt 7.4.2.4 overfor viser, er det gjort en betydelig innsats for å øke bevisstheten om personvern i politiet.

7.4.7.1 Håndtering av digitale beslag og overskuddsinformasjon

Vedrørende kommisjonens beskrivelse av problemstillingen knyttet til bortfiltrering av materiale, vil Kripos understreke at denne utfordringen henger tett sammen med innholdet i begrepet "sakens dokumenter" i straffeprosessloven §§ 242 og 264 og det tilhørende innsyn i dette materiale for sakens parter. Grovt sett er situasjonen prosessuelt i dag slik at alt materiale som tilkommer politiet som del av en etterforsking blir del av sakens dokumenter med den følge at materialet også som hovedregel skal gjøres tilgjengelig for sakens parter. Dette gjelder som utgangspunkt uavhengig av om politiet finner det relevant for etterforsking av saken og derfor har gjennomgått det. Hva særlig gjelder store digitale datamengder som tilkommer en etterforsking kan dette være utfordrende, herunder i forhold til personvernhensyn. Det vil i mange tilfelle være mindre og avgrensede deler av det totale materiale som er av interesse for etterforskingen og som politiet vil undersøke innholdet av. Det øvrige vil i utgangspunktet være etterforskingen uvedkommende og bør da – forutsatt at politiet ikke har gjennomgått det – også kunne unntas fra det materiale som utgjør "sakens dokumenter" og som sakens parter skal få innsyn i. Det presiseres imidlertid at politiet på vanlig måte må få anledning til å avklare hvilke deler av det innhentede materiale som kan være av interesse for etterforskingen og som man ønsker å gjennomgå, før øvrige deler "filtreres bort". De deler politiet finner av interesse må da også inngå i "sakens dokumenter" og derved gis innsyn i for sakens parter, jf. hensynet til kontradiksjon.

7.4.7.2 Utlevering av dokumenter til advokater

Kripos har – som det også vises til i dette punkt – lenge engasjert seg i den utfordring som ligger i manglende kontroll med spredningen av opplysningene i en straffesak etter at disse er utlevert sakens parter. Dette er fra Kripos side tatt opp flere ganger også med Kontrollutvalget for kommunikasjonskontroll hva gjelder materiale fra skjult tvangsmiddelbruk. At sakens parter må ha tilgang til materiale bestrides på ingen måte. Derimot innebærer deler av dagens praktisering av slik tilgang at man i realiteten har liten kontroll på hvem som får tilgang til materialet etter at det distribueres fra politiet. Som redegjort for under punkt 7.4.7.1 vil "sakens dokumenter" i mange tilfelle kunne utgjøre svært store mengder opplysninger – og også da opplysninger av svært personsensitiv karakter. Materiale vil i mange tilfelle også bestå av store deler "overskuddsinformasjon" i den forstand det berører andre forhold og/eller andre personer enn de som er involvert i saken.

Som kommisjonen, mener derfor også Kripos at man bør arbeide for en teknisk løsning som sikrer tilgang til (ikke utlevering av) straffesaksopplysninger til sakens parter.

Med hilsen

Ketil Haukaas
assisterende sjef Kripos

Dokumentet er elektronisk godkjent uten signatur.

Saksbehandler:
Jarle Langeland
seniorrådgiver