UiO : Det juridiske fakultet

Personvern vs. kriminalitetsbekjempelse

Et dokumentstudie med utgangspunkt i NOU 2003:21

Kandidatnavn: Øystein Balstad

Dato levert: 06/03.2018

Antall ord: 29212

Innholdsfortegnelse

Forord

Etter en noe lengre skriveprosess enn først antatt er jeg endelig ferdig. Selv om tematikken i denne oppgaven ikke var mitt førstevalg, har oppgavens problemstillinger og arbeidet med dem vokst på meg underveis i skriveprosessen. Som hos de fleste har motivasjonen variert gjennom arbeidet med masteroppgaven, og tidvis har jeg ikke sett lyset i enden av tunnelen. Heldigvis har jeg hatt flere gode personer i livet mitt som har motivert meg når arbeidet synes både for stort og til dels umulig. Jeg vil rette en stor takk til min kjære samboer og forlovede som ikke bare har holdt ut sammen med meg i denne perioden, men også vært en pådriver for å få masteroppgaven ferdig. Samtidig har både mine foreldre og mine svigerforeldre bidratt til å lette byren når det stod på som værst. Det er jeg evig takknemlig for!

Når jeg nå har kommet til veis ende med arbeidet må jeg også rette en takk til veilederen min, Tommy Tranvik. Din tålmodighet og veiledning har uten tvil ført meg hit jeg er kommet idag.

Jeg må også rette en takk til Senter for Rettsinformatikk ved Universitetet i Oslo. Hos dere er dørene alltid åpne og den faglige styrken som befinner seg på SERI har gitt meg et godt grunnlag for å skrive denne masteren.

Sist, men ikke minst, har tiden sammen med datteren min vært etterlengtede friperioder fra skrivingen.

Nå venter livet, et liv med nye utfordringer og mer læring. Jeg ser frem til å bidra med min kunnskap i arbeidslivet og jeg er overbevist om at Forvaltningsinformatikk er og blir et viktig fagfelt i fremtiden.

«Arguing that you don't care about the right to privacy because you have nothing to hide is no different than saying you don't care about free speech because you have nothing to say.»

- Edward Snowden

1 Introduksjon

Den 1.7.2014 trådte en ny politiregisterlov[1] i kraft, mer enn 10 år etter at initiativet til ny lov ble tatt. Den nye politiregisterloven erstattet strafferegistreringsloven[2] fra 1971.

Årsakene til en ny politiregisterlov var blant annet et økt behov for å samordne politiets bruk av personopplysninger, den økte bruken av IKT-løsninger i forbindelse med politiets arbeid og en relativt fragmentert ansvarsstruktur i justissektoren, særlig i politiet[3].

Fra før var politiets behandling av personopplysninger i liten grad lovregulert, og i den grad det var regulert var det gjennom instrukser eller rundskriv fra Politidirektoratet og Justisdepartementet. Dette fremstår som en lite oversiktlig måte å håndtere et så viktig område på, og i tillegg til dette er denne typen regulering sjelden tilgjengelig for offentligheten i den grad en lov er. En lovregulering av politiets behandling av personopplysninger vil således gi bedre forutberegnelighet, både for den registrerte og for politiet og påtalemyndigheten selv[4].

Lovens regulering av politiets behandling av personopplysninger innbefatter i stor grad politiets IKT-systemer, og særlig politiregistrene. Fra tidligere var politiets IKT-systemer i stor grad preget av alderdom, mangel på interoperabilitet[5] og lite fleksibilitet. Mange av registrene daterer seg langt tilbake i tid, og datasystemene som håndterer disse registrene likeså.

Til slutt er lovreguleringen tiltenkt å gi en mer oversiktlig ansvarsstruktur innen politi- og justissektoren. Med dette menes en tydelighet rundt hvem som har ansvaret for politets registre, hvem skal sørge for god internkontroll, hvem skal føre tilsyn med politiets behandling av personopplysninger, og så videre[6].

Det første steget på veien mot en ny politiregisterlov var Politiregisterutvalgets utredning. Denne ble ferdigstilt i 2003 og fikk navnet «Kriminalitetsbekjempelse og personvern[7]». Allerede i utredningens tittel setter utvalget fingeren på et spenningsforhold – kan politiet effektivt bekjempe kriminalitet og samtidig ivareta den enkeltes rettigheter og personvern?

Personvern og vern av personopplysninger står sentralt i denne oppgaven. Disse to begrepene kan se ut til å ha samme meningsinnhold, og i praksis er nok ikke koblingen mellom dem så fjern. Det foreligger likevel nyanseforskjeller mellom personvern og vern av personopplysnin-

1 Justis- og beredskapsdepartementet, "Politiregisterloven."

2 Justis- og beredskapsdepartementet, "Strafferegistreringsloven."

3 Justis- og politidepartementet, JD, "NOU 2003:21."

4 Ibid. Kapittel 2.3

5 Direktoratet for forvaltning og IKT, "Interoperabilitet - overordnet arkitekturprinsipp."

6 Ibid. Kapittel 2.3 og 3.3

7 Justis- og politidepartementet, JD, "NOU 2003:21."

ger. Personvern er å oppfatte som en generell rettighet for alle mennesker. Den enkelte har således en rett til å kunne verne om seg selv, sin kropp, sine tanker, sitt intellekt, sin eiendom og hjem. Vern av personopplysninger er en slags «gren på personverntreet» som omhandler den enkeltes rett til å ha kontroll på opplysninger om seg selv, hvordan disse opplysningene brukes og hvem som har tilgang til dem mv. Her skilles det oftest mellom sensitive- og ikke-sensitive personopplysninger. De sensitive personopplysningene har et noe strammere vern enn de ikke-sensitive.

Nyanseforskjellen mellom personvern og vern av personopplysninger er således at personvern dreier seg om overordnede prinsipper, en generell rettighet, mens vern av personopplysninger omhandler den enkeltes rett til å ha kontroll på opplysninger om seg selv. Felles for begrepene er at de begge omhandler vern av den personlige integritet.

Flere forskere har tidligere omtalt forholdet mellom kriminalitetsbekjempelse og personvern. Ingvild Bruce og Geir Sunde Haugland har skrevet om dette spenningsforholdet i artikkelsamlingen «Overvåking i en rettsstat[8]». De omtaler følgende i sin artikkel: *«Myndighetens metoder for å beskytte samfunnet og enkeltmennesker mot kriminalitet kan innebære inngrep i befolkningens grunnleggende rettigheter, og da særlig retten til privatliv, personvern og kontroll over opplysninger om en selv. Beroende på hvordan myndighetens tiltak er innrettet, vil de ikke bare ramme personer som er mistenkt for straffbare handlinger, men også utenforstående tredjepersoner eller befolkningen generelt. Videre aktualiserer slike inngrep spørsmål knyttet til om befolkningens rettssikkerhet ivaretas på en god nok måte ved bruk av slike former for statlig kontroll. Ivaretakelse av personvern og rettssikkerhet er forutsetninger for et samfunn basert på menneskeverd og demokrati. Myndighetens evne til å sørge for befolkningens sikkerhet og beskyttelse mot kriminelle handlinger er imidlertid også en forutsetning for et slikt samfunn. Verken personvernet eller kravet på rettssikkerhet kan derfor defineres som absolutte størrelser, men må, i hvert enkelt tilfelle, veies opp mot de verdier som begrunner det aktuelle inngrepet.[9]»*

Med utgangspunkt i høringsuttalelsene fra høringsrunden til NOU 2003:21 skal jeg forsøke å belyse høringsinstansenes syn på forholdet mellom personvern og kriminalitetsbekjempelse og hvordan dette skal håndteres i utformingen av lovgivningen. For å kunne gjennomføre dette vil jeg ta utgangspunkt i interesseteorien. Interesseteorien er en systematisert fremstilling av det som anses som personvern og vern av personopplysninger i dagens samfunn. Inter-

[8] Schartum, *Overvåking i en rettsstat*.

[9] Bruce, "Personvern, rettssikkerhet og vern mot alvorlig kriminalitet - Noen utgangspunkter." side 62/63

esseteorien består av ulike interesserer med tilhørende krav. Ved hjelp av interesseteorien kan jeg si noe om hvilke deler av interesseteorien høringsinstansene har lagt vekt på i sine uttalelser. I noen tilfeller kan det tenkes at høringsinstansenes argumenter knytter seg til ett eller flere av kravene i interesseteorien. Noen av høringsinstansene kan mene at personvern og vern av personopplysninger har fått for stor plass i lovforslaget, mens andre kan mene at kriminalitetsbekjempelsen og politiets oppgaver har fått for stor plass.

Ifølge en av mine kildepersoner er Politiregisterloven i behov av revisjon av flere årsaker. Blant annet, og mest relevant for oppgaven, er balansen mellom kriminalitetsbekjempelse og personvern ikke optimal slik den er idag. Ifølge kildepersonen har Politiet og påtalemyndigheten fått for vide adganger til behandling av personopplysninger gjennom Politiregisterloven, og personvernet har fått lide. Med dette i mente er det interessant å se hvilke vurderinger som ble gjort i utredningen og hvilke bemerkninger høringsinstansene hadde til lovforslaget og forholdet mellom kriminalitetsbekjempelse og personvern.

1.1 Problemstilling

Med utgangspunkt i NOU 2003:21 og høringsuttalelsene fra utredningens høringsrunde skal jeg belyse hva høringsinstansene mente om forholdet mellom personvern og kriminalitetsbekjempelse. Videre vil jeg anvende relevante deler av interesseteorien på høringsinstansenes uttalelser og på denne måten analysere hva de ulike høringsinstansene har lagt vekt på i forholdet mellom kriminalitetsbekjempelse og personvern. Dette munner ut i følgende to forskningsspørsmål;

1. Hvilke interesser i interesseteorien har høringsinstansene drøftet i sine merknader til forslaget til ny Politiregisterlov?
2. Hvilke synspunkter på forholdet mellom personvern og kriminalitetsbekjempelse kommer til uttrykk i høringsinstansenens drøftelser?

Problemstilling 1 vil jeg behandle i kapitlene 4-7, mens problemstilling 2 vil jeg behandle i underkapitlene 5.3, 6.3 og 7.3

1.1.1 Kjernepunkter fra høringsuttalelsene

Jeg har valgt meg ut tre kjernepunkter som jeg mener har betydning for utformingen av forslaget til ny Politiregisterlov. Disse tre kjernepunktene utgjør fundamentet for mine drøftinger og vil være de delene av lovforslaget jeg skal anvende teori på. Jeg har valgt disse tre kjernepunktene da de enten har elementer av personvern i seg eller har elementer av kriminalitetsbekjempelse i seg, eller en kombinasjon av personvern og kriminalitetsbekjempelse i seg. Vide-

re har jeg valgt disse tre kjernepunktene etter en gjennomgang av alle høringsinstansenes uttalelser og kommet frem til at hovedvekten av uttalelser har merknader til ett eller flere av kjernepunktene. De tre kjernepunktene er følgelig beskrevet kort nedenfor;

Pool-ordningen

- I NOU 2003:21[10] omtaler Politiregisterutvalget et tidsbegrenset unntak for kravene til formål, nødvendighet og relevans for politiet og påtalemyndigheten. Det er dette som er omtalt som Pool-ordningen. Utvalget skriver at *«(p)olitiet mottar opplysninger hvor de ikke har noen klar formening om til hvilket formål opplysningene kan komme til nytte, eller hvorvidt de er nødvendige og relevante for det formålet de er innhentet til(.)[11]».* Dette er gjerne knyttet til tips som tilkommer politiet fra publikum eller gjennom politiets egne obersvasjoner gjennom eksempelvis ordenstjenesten. Pool-ordningen gir som sådan politiet anledning til å behandle opplysninger som ikke er avklart, uten å måtte forholde seg til formålsbestemthet, nødvendighet eller relevans i en periode på inntil fire måneder. Utvalget bemerker at dette er nødvendig for å kunne opprettholde kriminalitetsbekjempelsen og at *«(f)or å bekjempe kriminalitet, er det nødvendig for politiet å ha bred tilgang til opplysninger, og ikke minst ha mulighet til å vurdere om disse er av betydning for deres arbeid.[12]»*
- Pool-ordningen har noen personvernmessige utfordringer. Personvernet er utfordrende å ivareta i en løsning som tillater fravikelse av grunnleggende personvernprinsipper som opplysningskvalitet, innsynsrett og formålsbestemt behandling av personopplysninger.

Politiattester

- Politiattester er definert av Politiregisterutvalget som *«bruk av opplysninger for å vurdere om en fysisk eller juridisk person er egnet til en bestemt stilling, funksjon, tillatelse, oppgave eller lignende.[13]»*
- Bruk av vandelskontroll og politiattester var tidligere hjemlet i spesiallovgivning, og da oftest gjennom bransjespesifikk lovgivning. Det vil si at hvis man skulle

[10] Justis- og politidepartementet, JD, "NOU 2003:21." Kapittel 13.7

[11] Justis- og politidepartementet, JD. Kapittel 13.7.1

[12] Justis- og politidepartementet, JD. Kapittel 13.7.1, andre avsnitt

[13] Justis- og politidepartementet, JD. Kapittel 15.1

arbeide innenfor luftfart, var det lovgivning knyttet til luftfart som regulerte bruk av vandelsattester. Det samme gjelder for vandelsattester knyttet til yrket som sykepleier, blant andre. Gjennom politiregisterloven er reguleringen av bruk av vandelsattester samlet i politiregisterloven, fremfor bransjespesifikk lovgivning.

→ Politiattester inneholder hovedsaklig personopplysninger, både sensitive- og ikke-sensitive som sådan. Personvern-prinsipper som konfidensialitet/taushetsplikt, innsynsrett og opplysningskvalitet er viktige i lys av politiattester som institusjon. Informasjonen i en politiattest kan medføre store skader på personvernet hvis den skulle komme på avveie eller bli kjent for uvedkommende. Likeledes vil informasjonen i en politiattest kunne avskrive noen fra å inneha en stilling, verv eller arbeid, noe som i seg selv er viktig for å ivareta spesifikke deler av samfunnet. Det er vel så viktig at informasjonen som fremstilles i en politiattest er basert på korrekte, oppdaterte og relevante opplysninger. Til slutt må den opplysningene gjelder ha mulighet til å bestride opplysningenes korrekthet.

Informasjonssikkerhet og sporbarhet

→ Informasjonssikkerhet dreier seg om *«tekniske og organisatoriske tiltak for å fremme en tilfredsstillende beskyttelse av opplysninger med hensyn til konfidensialitet, integritet og tilgjengelighet. Det er flere årsaker til at politiets behandling av personopplysninger må anses som en behandling med særlige sikkerhetsbehov. For det første behandles en rekke sensitive opplysninger i politiets systemer. For det andre vil det være mange som urettmessig ønsker å få tilgang til politiets systemer. Dette forsterkes ytterligere av at politiets «kunder» ikke er ukjente med å begå ulovlige handlinger for å oppnå det de ønsker. For det tredje er det svært mange som har tilgang til opplysninger i politiet, slik at den «interne trusselen» øker, i den forstand at faren øker for både hendelige uhell og uaktsomme og forsettlige overtredelser av regelverket.[14]»*

→ Sporbarhet[15] i elektroniske systemer er en løsning for å kunne logge brukeraktivitet, spesielt innenfor bruk av politiets elektroniske registre. Med sporbarhet kan den behandlingsansvarlige, eller andre med legitime interesser, se hva den enkelte bruker har søkt på eller lest av informasjon i registrene og videre avdekke hvorvidt vedkommende skal kunne ha tilgang til denne informasjonen eller ei. Sporbarhet i

[14] Justis- og politidepartementet, JD. Kapittel 18.4.1

[15] Justis- og politidepartementet, JD. Kapittel 18.5.1

elektroniske systemer skal således ivareta flere av Politiregisterlovens krav knyttet til informasjonssikkerhet, taushetsplikt, konfidensialitet og rettssikkerhet mv.

- *«Utvalget anbefaler at politiets informasjonssystemer, som da omfatter all elektroniske behandling av opplysninger, skal være sporbare. Dette vil i prinsippet være et kontrollerende tiltak i forhold til at reglene i politiregisterloven overholdes. I flere straffesaker har det vært problemer med lekkasjer, trolig fra politiet, og det har vist seg at kravet til tjenestelig behov for å innhente opplysninger ikke alltid respekteres. Politiregisterloven legger i utgangspunktet opp til forholdsvis stor frihet for politiet, og det er nødvendig å kunne kontrollere at reglene blir overhold. Det er dette som ligger i krav til «sporbarhet»*.[16]»

→ Informasjonssikkerhet og sporbarhet kan sees som verktøy for å ivareta personvernet når det kommer til behandling av personopplysninger i politiet og påtalemyndigheten. Særlig gjelder dette ivaretakelse og oppfyllelse av taushetsplikten, retten til innsyn, kvalitetssikring av opplysninger og ivaretakelse av lovverkets bestemmelser om retting, sperring og sletting samt ivaretakelsen av rettssikkerheten mv.

Med andre ord skal jeg analysere høringsinstansenes svar til lovforslaget for å finne ut hvordan de ser på ivaretakelsen av balansen mellom kriminalitetsbekjempelse og personvern i lovforslaget. I denne analysen av høringsinstansenes svar til lovforslaget skal jeg benytte interesseteorien, som presentert i kapittel 3.2, for å kunne sette høringsinstansenes uttalelser i sammenheng med de aktuelle personverninteressene som gjør seg gjeldende. På denne måten kan jeg kartlegge hvilke personvernutfordringer høringsinstansene mener at lovforslaget reiser eller om høringsinstansene mener at personvernet har fått for mye plass i lovforslaget sammenlignet med kriminalitetsbekjempelsen.

En kartlegging av arbeidet og vurderingene som ledet til den nye politiregisterloven er viktig av flere årsaker. For det første er politiet en av samfunnets aller mektigste myndighetsutøvere – en myndighetsutøver som befolkningen og samfunnet nærmest har full tillit til. Likevel foreligger det en del begrensninger for muligheten til å føre kontroll med hva politiet foretar seg når det kommer til behandling av personopplysninger. For det andre er det interessant å vite hva lovgiver har lagt vekt på når politiets bruk- og behandling av opplysninger skal lovreguleres og hvilke hensyn som har blitt tatt for å ivareta balansen mellom kriminalitetsbekjempelse

[16] Justis- og politidepartementet, JD. Kapittel 18.5.1, andre avsnitt

og personvern. Kan vi være sikre på at politiet til en hver tid behandler personopplysninger i tråd med gjeldende regelverk og er rettssikkerheten godt nok ivaretatt?

1.2 Lovgivningsprosessen

Utformingen av en ny lov i Norge består av flere prosesser og den endelige lovteksten kan være ulik det opprinnelige forslaget som et resultat av de ulike prosessene. Siden denne oppgaven i stor grad tar utgangspunkt i den delen av lovgivningsprosessen som omhandler offentlig høring, ser jeg det som viktig å gjøre kort rede for lovgivningsprosessen og særlig for hva en offentlig høring innebærer. I den følgende figuren nedenfor illustrerer jeg stegene i lovgivningsprosessen[17].

De fire første delene av prosessen, som vist i figuren ovenfor, kan summeres som forberedende lovarbeid;

- **Initiativ**
  - → *«I Norge viser det seg at initiativet i lovsaker oftest kommer fra forvaltningsorganer, særlig departementene, men også at interesseorganisasjoner spiller en viktig rolle. Stortingsorganer og stortingsrepresentanter kan ta lovinitiativ, men gjør det sjelden. Et initiativ følges i regelen opp enten ved at det nedsettes en utredningskomité, eller ved at et departement selv behandler saken.[18]»*
- **Behovsavklaring og utforming av mandat**

[17] Schartum, "Lovgivning: fra utredning til kunngjort lov." Figuren er min egen produksjon med utgangspunkt i Schartums forelesningsmateriale

[18] Bernt, "Lovgivning." Siste avsnitt

- → Et mandat[19] er et *oppdrag* eller en *fullmakt*. I lovgivningsprosessen betyr dette en beskrivelse av det som skal utredes, hvem som skal utrede saken, hva som skal fokuseres på, når utredningen skal leveres mv.
- → Utformingen av mandatet og behovsavklaringen gir visse retningslinjer for hva den nye loven skal inneholde og hvilket behov den er ment å dekke.

- **Utredning**
  - → *«Norges offentlige utredninger (NOU) er en fellesbetegnelse på statlige rapporter som har som formål å presentere og drøfte kunnskapsgrunnlaget og mulige handlingsvalg eller strategier for utvikling og iverksetting av offentlige tiltak for løsning av samfunnsmessige problemer og utfordringer.[20]»*
  - → Det er i denne delen av prosessen at det initielle forslaget til ny lov blir laget som en del av utredningen.
- **Offentlig høring**
  - → *«Høyring nyttar ein for at innbyggjarar, organisasjonar og næringsliv skal få seie si meining og kunne føre kontroll med kva forvaltninga gjer og korleis ho utfører oppgåvene sine. Ein sender saker på høyring av di det er ein demokratisk rett for alle å få vere med på å utforme offentleg politikk og av di synspunkta for dei som sakene kjem ved, skal verte kjende for dei som skal fatte avgjerder. Høyringssaker kan dreie seg om framlegg til lover og forskrifter som regulerer folk sine rettar og plikter, organisering av forvaltninga, endra myndeområde og utgreiingar.[21]»*

Etter at lovforslaget har vært på høring og aktuelle endringer har blitt vurdert og implementert i lovverket, blir forslaget oversendt Stortinget som vedtar loven. Vedtaket tas til Kongen i statsråd hvor Kongen signerer på lovvedtaket, og statsministeren kontrasignerer. Dette er per idag en ren formalitet, da Kongen ikke lenger har noen politisk makt[22]. Etter at loven er sanksjonert sendes den tilbake til det fagorganet som har ansvaret for lovforslaget og det er det ansvarlige departementet som gjør loven gjeldende. Til sist publiseres loven iht. Lov om norsk Lovtidend[23].

---

19 Hoel Lie, "mandat – avtale."

20 Hansen, "Norges offentlige utredninger (NOU)."

21 Regjeringa.no, "Kva er ei høyring?"

22 Stortinget, "Lovarbeidet." Niende avsnitt

23 Justis- og beredskapsdepartementet, "Lov om Norsk Lovtidend."

Lovgivningsprosessen, som vist ovenfor, er regulert av Utredningsinstruksen[24]. Denne instruksen er å anse som et verktøy for forvaltningen når det skal foretas reformer, regelendringer eller investeringer mv. Kapittel 3-3 i Utredningsinstruksen[25] omtaler den delen av lovgivningsprosessen som gjelder høringer. En offentlig høring, i dette tilfellet av NOU 2003:21, er ment for å ivareta retten til deltakelse i et demokratisk samfunn. Høringen gir samfunnet anledning til å kommentere og til dels påvirke utformingen av lovverket og på denne måten utøve sin rett til deltakelse. I tillegg har høringen en kontrollfunksjon – samfunnet kan føre kontroll med Regjeringens- og Stortingets virke. Til slutt ivaretar en offentlig høring prinsippene knyttet til offentlighet og gjennomsiktighet i forvaltningen.

Utredningsinstruksen[26] stipulerer unntak fra den generelle regelen om offentlig høring[27].

Høringsprosessen går ut på at den offentlige utredningen (NOU 2003:21) sendes til ulike aktører. Dette kan være departementer, direktorater, spesialorganer, næringsliv, interesseorganisasjoner mv. Det settes en høringsfrist, vanligvis ikke mindre enn 6 uker og normalt 3 måneder[28], og de ulike høringsinstansene må utferdige en uttalelse innen denne tidsfristen. I visse tilfeller kan tidsfristen utvides i samråd med det ansvarlige departementet[29]. Høringsuttalelsen følger ingen fastsatt mal og det er høringsinstansene selv som bestemmer form og innhold i sin uttalelse. Innen tidsfristen overleveres høringsuttalelsen skriftlig til det ansvarlige departementet og tas videre til behandling i departement og regjering.

1.3 Metode og datagrunnlag

Datagrunnlaget for denne oppgaven baserer seg hovedsaklig på offentlig tilgjengelige dokumenter. Jeg har begjært og fått innsyn i høringsuttalelsene fra høringen til NOU 2003:21 fra Justis- og Beredskapsdepartementet. Ut fra høringsrunden kom det 40[30] uttalelser etter at omtrent 70 instanser fikk tilbud om å uttale seg. De 40 uttalelsene kom hovedsaklig fra direktorater, departementer og politietaten. I tillegg var det noen organisasjoner, foreninger og tilsynsmyndigheter som uttalte seg.

[24] Finansdepartementet, "Utredningsinstruksen." (merk at gjeldende Utredningsinstruks er fra 2016, hvor den forrige Utredningsinstruksen er fra 2000 og videre revidert i 2005.)

[25] Finansdepartementet. Kapittel 3-3

[26] Finansdepartementet. Kapittel 3-3, andre avsnitt

[27] Høring kan unnlates dersom den ikke vil være praktisk gjennomførbar, dersom den kan vanskeliggjøre gjennomføringen av tiltaket eller må anses som åpenbart unødvendig.

[28] Finansdepartementet, "Utredningsinstruksen." Kapittel 3-3

[29] Det finnes ingen formalitet rundt utsatt høringsfrist. Skulle en høringsinstans ønske utsatt høringsfrist gjøres dette i direkte samråd med det ansvarlige departementet, gjerne via telefon eller e-post. Det er i departementets interesse å få saken så godt opplyst som mulig, og således kan absolutte frister være mindre hensiktsmessig sammenlignet med en utvidet frist som kan gi en bedre opplyst sak.

[30] Justis- og politidepartementet, "Ot.prp.nr.108 (2008-2009)." Kapittel 2.3

Jeg ikke har fått utlevert alt jeg har bedt om innsyn i når det kommer til høringsuttalelser. Hvorvidt dette er en forglemmelse fra Justisdepartementets side vites ikke. Dette gjelder to høringsuttalelser; Konfliktrådet (for Sandnes mv) og Norsk forening for kriminal reform (KROM). Jeg kan ikke vite sikkert hva disse høringsuttalelsene inneholder, da jeg ikke har lest dem i sin helhet. Ut fra Ot.prp.nr.108 (2008-2009)[31] kan jeg lese at Konfliktrådet (for Sandnes mv) kun nevnes en gang[32] under høringsinstansenes syn, mens Norsk forening for kriminal reform (KROM) nevnes i flere[33] av kapitlene med tilsynelatende kritiske uttalelser knyttet til lovforslaget. KROM later likevel til å ikke ha fått sine betraktninger særlig hensyntatt i utformingen av lovforslaget. Som et hovedpunkt kan det nevnes at KROM anser at kriminalitetsbekjempelsen har fått for stor plass i lovforslaget sammenlignet med personvernet og at politiet og påtalemyndigheten har fått for vide adganger til å samle inn og behandle personopplysninger.

Disse to høringsuttalelsene velger jeg å ikke vie særlig oppmerksomhet i min fremstilling da jeg ikke har lest dem i sin helhet.

De øvrige høringsuttalelsene vil gi et bilde på hvordan de ulike instansene stilte seg til lovforslaget, hva som var viktig for den enkelte instans i utformingen av lovforslaget og hvordan høringsinstansene mente at forholdet mellom personvern og kriminalitetsbekjempelse skulle best ivaretas. Høringsinstansene representerer ulike deler av forvaltningen og næringslivet og bemerker i sine uttalelser både like og ulike momenter knyttet til lovforslaget. Høringsuttalelsene viser videre hvilke aktører som fremmet hvilke synspunkter og om en viss aktørgruppe kan sies å ha sammenfallende synspunkter på bakgrunn av hvilken sektor de hører til. Høringsuttalelsene sier også noe om hvem som har hvilke interesser i det nye lovforslaget.

Jeg anvender juridisk metode for å analysere lovforslaget til ny politiregisterlov og for å redegjøre for de bestemmelsene fra lovverket som er aktuelle for oppgavens omfang. Jeg må også kunne si å anvende juridisk metode for å forstå enkelte deler av høringsuttalelsene og sette dem i sammenheng med lovforslaget.

Jeg bruker videre dokumentstudie som metode for å analysere innholdet av høringsuttalelsene fra høringsrunden til NOU 2003:21. Dette inngår i samfunnsvitenskapelig metode hvor jeg gjennomgår og analyserer høringsinstansenes svar til lovforslaget. Inkludert i dette tilkommer

[31] Justis- og politidepartementet.

[32] Ibid. Kapittel 12.7.3

[33] Ibid. Kapitlene 7.1.2, 9.2.4, 9.4.4, 9.7.2, 11.8.4, 11.11.3, 11.12.3, 11.13.4, 11.14.2, 12.1.3, 13.2.4, 14.4, og 14.6.2

intervjuene jeg gjennomførte hos KRIPOS og Oslo Politidistrikt i forbindelse med forprosjekt-trapporten til mastergradoppgaven.

Jeg har lest og gjennomgått de høringsuttalelsene jeg fikk innsyn i fra høringsrunden til NOU 2003:21 og sortert ut hvilke aktører som fremmet hvilket synspunkt i tilknytning til de temaene jeg ønsker å se nærmere på i denne oppgaven. Noen aktører er mer fremtredende enn andre, både i mengde og type synspunkter som ble fremmet. Dette gjelder særlig politietaten som har gitt uttalelse fra flere politidistrikter, særorganer, påtalemyndigheten, direktorat og interesseorganisasjoner. Det er ikke så rart at politietaten selv har synspunkter knyttet til et lovverk som er ment å regulere deres arbeid, og derav kommer nok mengden og antall synspunkter fra politietaten inn i bildet.

De høringsuttalelsene som kommenteres og drøftes i kapitlene 5 til 7 er tatt med i mine vurderinger nettopp fordi de har synspunkter knyttet til ett eller flere av mine kjernepunkter eller personverninteresser. De må således ansees som relevante for problemstillingen. De høringsuttalelsene som er utelatt fra mine drøftinger og analyser er utelatt da de ikke inneholder relevante synspunkter i forhold til problemstillingen min.

Det hefter noen utfordringer knyttet til det å føre rene dokumentstudier uten utstrakt bruk av andre metoder for datainnsamling. Ved å studere dokumenter knyttet til lovgivningsprosessen baserer jeg meg på primærkilder[34] – altså originalt materiale. Kildene jeg baserer min oppgave på er å anse som offentlige og/eller institusjonelle – altså ment for publisering i offentligheten og skrevet av kollektive enheter. Det blir likevel mine tolkninger av disse kildene som fremstilles i oppgaven.

Jeg gjorde tidlig forsøk på å få til dybdeintervjuer med aktuelle kilder, men dette viste seg etterhvert å være vanskelig å gjennomføre. Som en konsekvens av dette får oppgaven et breddepreg fremfor et dybdepreg.

1.4 Kapitteloversikt

I det følgende vil jeg gjøre kort rede for innholdet i hvert enkelt hovedkapittel.
Kapittel 2 gjør rede for politiets virksomhet, prosessen fra Utredningen (NOU 2003:21) til Lovvedtak 38, en fremstilling av Politiregisterloven og dens formål, samt reglene knyttet til oppgavens tre kjernepunkter (pool-ordningen, politiattester og informasjonssikkerhet/sporbarhet).
Kapittel 3 er et teorikapittel som gjør rede hvor hva personvern er, for hva interesseteorien er og hvordan denne teorien skal brukes videre.

[34] Tranvik, "Dokumentstudier, innholdsanalyse og narrativ analyse."

Kapitlene 4 til 7 er drøftingskapitler hvor teori møter empiri. Dette innebærer også beskrivelse av høringsinstansenes merknader til lovforslaget, samt vurderinger av hvilke interesser fra interesseteorien som drøftes i merknadene. I tillegg kommer en vurdering av hvorvidt det er kriminalitetsbekjempelse eller personvern som vektlegges i høringsinstansenes uttalelser. Her besvares også problemstillingene som oppgaven tar for seg.
Kapitlene 8 er oppsummeringskapitler hvor den andre problemstillingen besvares.

2 Politiets virksomhet, registre og lovverk

I det følgende kapittelet gir jeg en fremstilling av hva politiets virksomhet innebærer. Videre gjør jeg rede for politiets ulike registerkategorier og hva de ulike registrene inneholder av opplysninger. Til slutt gjør jeg rede for hva Lovvedtak 38 inneholder i kapittel 2.3, med særlig fokus på de delene av lovverket jeg skal ta for meg videre i oppgaven.

2.1 Politiets virksomhet

Som kjent er politiets oppgaver heterogene, men med en hovedvekt på bekjempelse av kriminalitet og opprettholdelse av den alminnelige ro og orden i samfunnet. I tillegg består en stor del av politiets arbeid i tjenesteproduksjon og forvaltningsmessige arbeidsoppgaver. For å kunne si noe om politiets registre og lovreguleringen av disse, må en se på politiets virksomhet under ett. Dette grunner i at Politiet har tre hovedkategorier av registre; administrative registre, forvaltningsregistre og registre til bruk i kriminalitetsbekjempelsen. Innenfor registre til bruk i kriminalitetsbekjempelsen finnes det ytterlige tre kategorier av registre; reaksjonsregistre, operative registre og saksbehandlingsregistre. Med dette i bakhodet kan man gjenfinne disse ulike kategoriene av registre i den følgende figuren fra NOU 2003:21[35].

<table>
<tr><td colspan="7">Politiets virksomhet</td></tr>
<tr><td colspan="5">Politimessige / polisiære oppgaver</td><td rowspan="2">Politiets forvaltnings-oppgaver</td><td rowspan="2">Politiets sivile oppgaver</td></tr>
<tr><td colspan="3">Kriminalitetsbekjempelse</td><td colspan="2">Annen virksomhet</td></tr>
<tr><td>Straffesak</td><td>Fore-byggende virksomhet</td><td>Ordens-tjenesten</td><td>Service-funksjon</td><td>Hjelpe-funksjon</td><td>Bistands-funksjon</td><td></td><td></td></tr>
</table>

Illustrasjon 1

Som figuren ovenfor viser er politiets virksomhet delt inn i tre deler; politimessige oppgaver, forvaltningsoppgaver og sivile oppgaver. Politiets oppgaver er nærmere regulert og gjengitt i Politilovens § 2[36], og kan således sees som bakgrunnen for figuren. Politiregisterloven[37] stipulerer i § 3, under lovens virkeområde, at politiets forvaltningsoppgaver[38] og sivile oppgaver ikke er omfattet av Politiregisterloven. Dette etterlater de politimessige oppgavene som vist til venstre i figuren.

---

35 Justis- og politidepartementet, JD, "NOU 2003:21." Kapittel 3.5.2

36 Justis- og beredskapsdepartementet, "politil."

37 Justis- og beredskapsdepartementet, "Politiregisterloven." §3

38 Unntaket gjelder for Politiets Sikkerhetstjeneste og deres forvaltningsoppgaver som er omfattet av Politiregisterloven

Politiets forvaltningsoppgaver går eksempelvis ut på utstedelse av pass og utstedelse av våpenkort. Politiets forvaltningsoppgaver er omfattende og de ulike forvaltningsoppgavene er hjemlet i mer enn 100[39] forskjellige lovverk.

Politiets sivile oppgaver er svært ulike i karakter. Eksempler på politiets sivile oppgaver er å melde pårørende om dødsfall, gjennomgå dødsbo med arvinger og frata personer eiendeler de ikke har klart å betale for gjennom namsmanns-ordningen.

Når det kommer til de polisiære oppgavene er de inndelt i to kategorier; kriminalitetsbekjempelse og annen virksomhet. Annen virksomhet omfatter blant annet utstedelse av vandelsattester og behandling av innsynsbegjæringer med mer. Den andre delen av de polisiære oppgavene er kriminalitetsbekjempelse. Dette omfatter politiets forebyggende virksomhet, ordenstjenesten og gjennomføring av straffesaker.

Daværende rektor ved Politihøgskolen, Håkon Skulstad, skrev i 2011 et innlegg[40] i Lensmannsbladet om forebyggende virksomhet og skriver følgende;

«Forebygging handler om å hindre at noen begår straffbare handlinger (proaktive tiltak) for første gang, eller at de gjør nye straffbare handlinger. Det innebærer at det kan være aktuelt å forebygge med bruk av både proaktive og reaktive strategier (oppklaring og iretteføring av begått kriminalitet).»

Noe av det en husker best fra barndommen var de gangene en politimann besøkte skolen for å fortelle om rusmidler eller trafikksikkerhet mv. Dette er en av tiltakene som inngår i forebyggende virksomhet i en proaktiv form – altså å forsøke å forhindre lovbrudd gjennom kontakt med barn og unge. Det er også en slags forebyggende virksomhet at politiet har kontakt med ulike kriminelle miljøer og viser sin tilstedeværelse ovenfor dem. Dette kan bidra til å forhindre at kriminelle handlinger skjer. Politiet har forebyggende enheter som utelukkende jobber med forebyggende tiltak. Likevel tilfaller deler av den forebyggende virksomheten den enkelte polititjenesteperson gjennom ordenstjenesten. Ordenstjenesten beskrives lettest som det daglige politiarbeidet som gjerne foregår gjennom patruljering og tilstedeværelse ute blant befolkningen.

For å forstå hvorfor «straffesak» er mørklagt i figuren ovenfor må man se på Politiregisterlovens § 5 om nødvendighetskravet. Når opplysningene som behandles er en del av en straffesak er det straffeprosessloven[41] som er hjemmelsgrunnlaget. Utenfor straffesak og i

[39] Justis-og politidepartementet, "Politireform 2000 Et tryggere samfunn." Kapittel 3.3.5 tredje avsnitt

[40] Skulstad, "Hvordan forebygge mer og bedre?" side 24

[41] Justis- og beredskapsdepartementet, "Strpl."

kriminalitetsbekjempende hensikt kan opplysninger behandles etter politiregisterlovens bestemmelser. En må altså skille mellom når opplysninger behandles i en straffesak, eller utenfor en straffesak i kriminalitetsbekjempende hensikt.

2.2 Politiets registre

Per idag finnes det 19 politiregistre hvorav Kriminalpolitisentralen (KRIPOS) er behandlingsansvarlig for 17 av dem. De to resterende politiregistrene, hvitvaskingsregisteret[42] og Politiets utlendingsregister[43], er tillagt henholdsvis ØKOKRIM og Politiets Utlendingsenhet som behandlingsansvarlig. Dette fremkommer av Politiregisterforskriften[44] og hvert enkelt av registrene er detaljregulert gjennom denne forskriften. Politiregisterloven hjemmelsfester[45] politiets opprettelse og bruk av politiregistre, og detaljregulerer således ikke hvert enkelt av politiregistrene.

Ifølge Politiregisterutvalget[46] deles politiregistrene inn i tre hovedkategorier[47]; administrative registre, forvaltningsregistre og registre til bruk i kriminalitetsbekjempelsen.

De administrative registrene er hovedsaklig lønns- og personalregistre.

Forvaltningsregistrene brukes i forbindelse med politiets forvaltningsoppgaver, blant annet våpenregisteret og passregisteret. Forvaltningsregistrene er ikke tatt inn som en del av registre til bruk i kriminalitetsbekjempelsen, men ikke sjelden kan opplysninger fra forvaltningsregistrene brukes i kriminalitetsbekjempende hensikt. Formålet med forvaltningsregistrene er likevel ikke å oppfylle kriminalitetsbekjempende formål, men oppfyllelse av politiets forvaltningsoppgaver, og de er derfor oppstilt som en egen kategori av registre.

Registre til bruk i kriminalitetsbekjempelsen er den mest heterogene gruppen av politiregistrene og omfatter et vidt spekter av opplysninger og bruksområder. Politiregisterutvalget deler disse registrene inn i tre underkategorier på følgende måte[48]; reaksjonsregistre, saksbehandlingsregistre og operative registre.

I reaksjonsregistrene lagres opplysninger om reaksjoner politiet har ilagt noen på bakgrunn av en straffbar handling. Dette strekker seg fra bøteleggelser til rettskraftige dommer i strafferettspleien. De mest sentrale registrene av reaksjonsregistrene er bøteregisteret (BOT)

[42] Justis- og beredskapsdepartementet, "Politiregisterforskriften." Kapittel 52

[43] Justis- og beredskapsdepartementet. Kapittel 56

[44] Justis- og beredskapsdepartementet. Del 11

[45] Justis- og beredskapsdepartementet, "Politiregisterloven." Kapittel 3

[46] Justis- og politidepartementet, JD, "NOU 2003:21."

[47] Justis- og politidepartementet, JD. Kapittel 4.2.2

[48] Justis- og politidepartementet, JD. Kapittel 4.2.2, fjerde avsnitt

og Det sentrale straffe- og politiopplysningsregisteret (SSP). I BOT registreres forelegg, bøter gitt ved dom, samt saksomkostninger, erstatninger og inndragninger knyttet til dom. SSP omfatter Reaksjonsregisteret[49] og Personidentitet- og politiopplysningsregisteret[50] og inneholder en betydelig mengde opplysninger. Nedenfor følger en oversikt over hvilke opplysninger som kan registreres i henholdsvis Reaksjonsregisteret og Personidentitet- og politiopplysningsregisteret, som tilsammen utgjør Det sentrale straffe- og politiopplysningsregisteret (SSP).

Reaksjonsregisteret	**Personidentitet- og politiopplysnings-registeret**
dom på betinget og ubetinget fengsel	navn, oppnavn og aliasnavn
dom på forvaring, eventuelt sikring	fødselsnummer og kjønn
dom på samfunnsstraff, eventuelt samfunns-tjeneste	statsborgerskap, fødested og fødeland
dom på ungdomsstraff	adresse- og kontaktinformasjon mv.
dom eller vedtatt forelegg på betinget og ubetinget bot	andre ID-er, som for eksempel referanse til utlendingssak, utenlandsk ID, fiktive og mis-brukte identiteter
dom på rettighetstap	signalement; herunder utseende og særkjenne
dom og forelegg på militær arrest	informasjon om registrert biometri (foto, DNA, fingeravtrykk med mer)
betinget dom hvor fastsetting av straff utstår	øvrige opplysninger fra personaliarapporten i den grad det anses nødvendig
påtaleunnlatelse etter straffeprosessloven § 69 og § 70	foretaksinformasjon
overføring til behandling i konfliktråd	melding om anmeldelse mot person eller fore-tak
overføring til tvunget psykisk helsevern eller tvungen omsorg, eventuelt sikring	tiltak som gir den registrerte status som siktet i straffesak
overføring til barneverntjenesten	opplysning om at person er etterlyst
inndragning	opplysning om at det er gjennomført bekym-ringssamtale
tap av retten til å føre motorvogn mv. og tap av retten til å drive persontransport mot ved-	rettskraftig avgjørelse av straffesaken

[49] Justis- og beredskapsdepartementet, "Politiregisterforskriften." §44-4

[50] Justis- og beredskapsdepartementet. § 49-4

erlag (kjøreseddel)	
dom eller vedtatt forelegg med straff-utmålingsfrafall	tidspunkt, varighet og lokasjon i forbindelse med pågripelse
personundersøkelse og beslutning om retts-psykiatrisk undersøkelse med eventuelle til-leggserklæringer. Registreringen begrenses til tidspunktet for undersøkelsen eller observa-sjonen, samt hvilke sakkyndige som har med-virket og resultatet av observasjonen.	tidspunkt, varighet og lokasjon i forbindelse med varetekt
eventuelle særvilkår knyttet til reaksjonen	beregnet varetektsfradrag
endring av avgjørelse som nevnt i første ledd[51], herunder ved gjenåpning, benådning eller ved brudd på fastsatte vilkår	informasjon om utvisning, bortvisning, utlevering og uttransportering, herunder opp-lysninger om varetekt etter forvaltningsvedtak om utvisning
fullbyrdelse av reaksjoner, herunder opplys-ninger om utsettelse, innsetting, overføringer, permisjoner og andre endringer, også om endring i beregning av reaksjonens varighet samt om løslating	informasjon om besøks- og oppholdsforbud, og om personer som skal beskyttes ved ilagt forbud
andre reaksjoner som er blitt registrert der i henhold til tidligere ordninger	melding om bøtesoning av forenklede forelegg
	informasjon om hvorvidt vedkommende har våpen
	informasjon om personer som er mistenkt el-ler siktet i samme sak

Som tabellen viser er SSP særdeles omfattende når det kommer til mengde og type opplysnin-ger som kan registreres, og opplysningene bærer preg av å være hovedsaklig sensitive person-opplysninger.

Saksbehandlingsregistrene har til hensikt å bistå politiet med å skape en oversiktlig og effek-tiv saksgang. Som et nav i saksbehandlingsregistrene står Basisløsninger[52] (BL). Mesteparten av den informasjonen som skal føres i ett eller flere av saksbehandlingsregistrene føres først i

[51] Ref. dom på betinget og ubetinget fengsel

[52] Justis- og politidepartementet, JD, "NOU 2003:21." Kapittel 4.10

BL og overføres derifra til det registeret opplysningene tilhører. Med dette menes, eksempelvis, at opplysninger som i utgangspunktet tilhører Straffesaksregisteret[53] (STRASAK) først føres i BL og overføres direkte fra BL til STRASAK. Det samme gjelder for Etterlysningsregisteret (Elys) og BOT. Saksbehandlingsregistrene inneholder informasjon om en sak helt fra den er anmeldt til saken er avsluttet.

Operative registre har til hensikt å gi en kronologisk oversikt over politiets operative virksomhet. Sentralt i de operative registrene står PolitiOperativt system (PO) som er politiets elektroniske vaktjournal. PO gir en døgnkontinuerlig oversikt over politiets operative virksomhet. Med dette menes at alle henvendelser og hendelser som forekommer i et politidistrikt registreres i PO og eventuelt omgjøres til et oppdrag for en politipatrulje. Inkludert i dette ligger planlagte oppgaver for den operative virksomheten, som eksempelvis transport av fanger, demonstrasjoner og veisperringer mv. På denne måten kan politiet bruke PO til å planlegge sin operative virksomhet og ha oversikt over ledige ressurser og den enkelte politibetjent kan rapportere inn hendelsesforløp på et oppdrag mv. Med hensyn til hvilke opplysninger som kan registreres i operative registre, og kanskje særlig PO, er det få begrensninger. Dette har sitt grunnlag i at de operative registrene er et arbeidsverktøy for politiet og en må således kunne registrere de opplysninger som ses nødvendig å registrere for å ivareta den operative virksomheten. Dette medfører at opplysningene som føres ikke alltid oppfyller et tradisjonelt kvalitetskrav, altså at opplysningene må være korrekte, oppdaterte og relevante. En henvendelse til politiet fra publikum registreres i PO som nettopp en henvendelse uten å nødvendigvis si noe om kvaliteten på opplysningene som kommer fra publikummeren. Det viktige er at opplysningene gjengis korrekt av den som mottar opplysningene.

2.3 Politiregisterloven – Lovvedtak 38 (2009-2010)

I det følgende kapittelet vil jeg presentere Politiregisterloven med utgangspunkt i Lovvedtak 38 (2009-2010)[54]. Jeg vil gi overordnede beskrivelser av lovverket og mer spesifikke beskrivelser av de delene av lovverket denne oppgaven baserer seg på, nærmere bestemt de delene av lovverket som regulerer pool-ordningen[55], politiattester[56] og internkontroll[57].

Lovvedtak 38 (2009-2010)[58] inneholder 13 kapitler og 70 paragrafer.

[53] Justis- og beredskapsdepartementet, "Politiregisterforskriften." Kapittel 48

[54] Justis- og beredskapsdepartementet, "Lovvedtak 38 (2009-2010)."

[55] Justis- og beredskapsdepartementet, "Politiregisterloven." § 8

[56] Justis- og beredskapsdepartementet. Kapittel 7

[57] Justis- og beredskapsdepartementet. Kapittel 4

[58] Justis- og beredskapsdepartementet, "Lovvedtak 38 (2009-2010)."

Kapittel 1 regulerer lovens formål, definisjoner og virkeområde.

Kapittel 2 regulerer krav til behandlingen av opplysninger.

Kapittel 3 regulerer politiets registre og andre systemer.

Kapittel 4 regulerer informasjonssikkerhet og internkontroll.

Kapittel 5 regulerer utlevering og tilgang til opplysninger.

Kapittel 6 regulerer begrensninger i taushetsplikten.

Kapittel 7 regulerer vandelskontroll og attester.

Kapittel 8 regulerer informasjonsplikt, innsyn, retting, sperring og sletting.

Kapittel 9 regulerer klageadgang og erstatning.

Kapittel 10 regulerer meldeplikt og tilsyn.

Kapittel 11 regulerer Politiets sikkerhetstjeneste.

Kapittel 12 regulerer forskrifter, mens kapittel 13 er sluttbestemmelser.

Lovens formålsparagraf[59] beskriver spenningsforholdet mellom personvern og kriminalitetsbekjempelse;

«Formålet med loven er å bidra til effektiv løsning av politiets og påtalemyndighetens oppgaver, beskyttelse av personvernet og forutberegnelighet for den enkelte ved behandling av opplysninger.»

Formålet med loven er således tredelt. Loven skal være et verktøy for politiet og påtalemyndigheten i deres arbeid. Loven, som verktøy, skal besørge effektive og formålstjenlige bestemmelser og rammer som ikke legger for vidtgående begrensninger for politiets- og påtalemyndighetens arbeid. Med andre ord bør ikke loven legge for vidtgående begrensninger for politiets mulighet til å bedrive kriminalitetsbekjempende virksomhet. På samme tid skal loven beskytte personvernet. Med beskyttelse av personvernet anses både den registrertes personvern og lovanvenders[60] personvern som like viktig. Dette viser seg best gjennom lovens oppbygning som i stor grad sammenfaller med oppbygningen av personopplysningsloven. Flere

[59] Justis- og beredskapsdepartementet. § 1

[60] Med lovanvender mener jeg personer som anvender Politiregisterloven i sitt daglige virke. Dette gjelder hovedsaklig polititjenestemenn, andre ansatte i politiet og påtalemyndigheten.

av de samme prinsippene og bestemmelsene som omhandler personvern er like i begge lovene. Som den tredje delen av formålet med loven står forutberegnelighet ved behandling av opplysninger. Med dette menes at loven skal være lett forståelig for enhver, både språklig og innholdsmessig. Det er ønskelig at loven som helhet skal gi både lovanvender og befolkningen mulighet til å gjøre seg kjent med hvilke regler som gjelder for politiets- og påtalemyndighetens behandling av opplysninger. Hvis loven er mulig å forstå for enhver vil den skape forutberegnelighet – altså en mulighet for den enkelte å forutse hvilke rettigheter, konsekvenser og plikter som er gjeldende.

Når det kommer til legaldefinisjoner inneholder Politiregisterloven hovedsaklig like definisjoner[61] som Personopplysningsloven, men det er lagt til seks[62] ekstra legaldefinisjoner som er spesifikt myntet på politiets behandling av opplysninger. Disse seks legaldefinisjonene er som følger;

- *ikke-verifisert opplysning:* opplysning som ikke er avklart
- *merking:* markering av lagrede opplysninger uten at hensikten er å begrense den fremtidige behandlingen av disse opplysningene
- *sperring:* markering av lagrede opplysninger i den hensikt å begrense den fremtidige behandlingen av disse opplysingene
- *straffesak:* sak som behandles etter straffeprosessloven
- *vandelskontroll*: bruk av opplysninger for å vurdere om en fysisk eller juridisk person er egnet til en bestemt stilling, virksomhet, aktivitet eller annen funksjon
- *politimessig formål*:
  - a) politiets kriminalitetsbekjempende virksomhet, herunder etterforskning, forebyggende arbeid og ordenstjeneste, og
  - b) politiets service- og bistandsfunksjon samt føring av vaktjournaler

Siden disse legaldefinisjonene er «nye» er en forklaring av hver enkelt legaldefinisjon viktig for å kunne forstå lovverket og hva som menes i den enkelte paragraf.
Definisjonen ikke-verifisert opplysning henspeiler direkte på pool-ordningen som er nedfelt i § 8. Det er nettopp ikke-verifiserte opplysninger som registreres i pool-ordningen.

[61] Legaldefinisjoner som er tilnærmet like i Personopplysningsloven og Politiregisterloven er definisjonene på personopplysning, behandling av opplysninger, register, behandlingsansvarlig, databehandler, registrert og samtykke.

[62] Justis- og beredskapsdepartementet, "Lovvedtak 38 (2009-2010)." § 2 nr. 8 tom. nr. 13

Definisjonen av politimessige formål henspeiler direkte på kravet til formålsbestemthet i § 4 som sier at opplysninger kan behandles til det formål de er innhentet for eller til andre politimessige formål.

Definisjonen av vandelskontroll er viktig da reguleringen av vandelskontroll og politiattester tidligere har vært lovfestet i andre lover eller gjennom ulike instrukser mv. Reguleringen av vandelskontroll i Politiregisterloven er første gang en slik regulering samles i ett lovverk, og definisjonen er således viktig for tolkningen av politiregisterlovens kapittel 7.

Bruken av merking og sperring av opplysninger er noe som tradisjonelt sett er lite brukt i personvernlovgivning. Mens Personopplysningsloven hovedsaklig bruker begrepene «retting og sletting», omtales også muligheten for «merking og sperring» av opplysninger. I de tilfeller, etter Personopplysningsloven, hvor merking eller sperring skal brukes er det Datatilsynet som bestemmer dette hvis «tungtveiende personvernhensyn tilsier det[63]». Politiet og påtalemyndigheten på sin side trenger ikke gå gjennom Datatilsynet for å merke eller sperre opplysninger – dette tilfaller den behandlingsansvarlige selv.

2.3.1 Pool-ordningen

Pool-ordningen, som er ett av kjernepunktene jeg skal ta for meg videre i oppgaven, reguleres i politiregisterlovens kapittel 2 § 8 som «Tidsbegrenset unntak fra kravene til formålsbestemthet, nødvendighet og relevans». Bestemmelsen sier at kravene til formålsbestemthet etter § 4, kravene til nødvendighet etter § 5 og kravene til opplysningenes relevans etter § 6 første ledd nr.1 kan fravikes på en periode inntil 4 måneder for å avklare om de overnevnte kravene er oppfylt. I denne perioden på 4 måneder kan opplysningene behandles uten å oppfylle kravene til formålsbestemthet, nødvendighet og relevans sålenge opplysningene ikke er en del av en straffesak. Iløpet av denne perioden på 4 måneder, og snarest mulig, skal opplysningene som behandles etter denne paragrafen underlegges kontroll for å avklare om opplysningene fyller kravene til formål, nødvendighet og relevans. Hvis de ikke fyller kravene, skal de slettes eller eventuelt behandles etter et annet rettslig grunnlag enn denne paragrafen.

Forsmålsbestemthetsparagrafen, som gjengitt i Politiregisterlovens § 4[64], sier at *«opplysninger kan behandles til det formål de er innhentet for eller til andre politimessige formål (..)»*. For å vite til hvilket formål en opplysning er innhentet, kan en henvende seg til Politiregisterforskriften[65] del 11 og se hvilket av registrene opplysningene tilhører og hvilket formål det enkelte register har. Når det kommer til formuleringen *«(..) eller til andre politimessige formål (..)»*

[63] Justis- og beredskapsdepartementet, "popplyl." § 27 andre og tredje ledd

[64] Justis- og beredskapsdepartementet, "Politiregisterloven." § 4

[65] Justis- og beredskapsdepartementet, "Politiregisterforskriften." Del 11, §§ 44-1 - 58-13

gjelder dette eksempelvis i de tilfeller hvor politiets annen virksomhet[66] krever gjenbruk av opplysninger som opprinnelig var innsamlet til et annet formål. Et konkret eksempel på dette er utstedelse av politiattester, hvor opplysningene som tidligere var behandlet til et annet formål nå skal behandles med det formål å produsere en politiattest.
Politiet og påtalemyndigheten gis vide adganger til hvilke opplysninger som kan behandles og til hvilket formål. Det må også bemerkes at de opplysningene som politiet og påtalemyndigheten behandler i stor grad vil falle inn under beskrivelsen «sensitive personopplysninger» fra Personopplysningsloven[67].

Nødvendighetsparagrafen[68], stipulerer at opplysninger bare kan behandles når det er nødvendig ut fra politimessige formål[69]. I den enkelte straffesak er det straffeprosessloven som regulerer behandling av opplysninger. Utenfor den enkelte straffesak kan det, etter nødvendighetsparagrafen, behandles opplysninger om personer som er tilknyttet et *«miljø hvor en vesentlig del av virksomheten består i å begå lovbrudd, eller ut fra andre holdepunkter kan antas å begå slike.»* Dette gjelder selv om vedkommende person er under den kriminelle lavalder. Det samme gjelder for personer som har særlig tilknytning til personer som er del av et miljø hvor en vesentlig del av virksomheten består i å begå kriminelle handlinger.
Det kan også behandles opplysninger om personer som har blitt utsatt for, eller sannsynligvis vil bli utsatt for, et lovbrudd. Til sist kan det behandles opplysninger om en person er informant.

Nødvendighetskravet fremkommer best i Menneskerettsloven artikkel 8[70] hvor det beskrives som at inngrepet må være *« (..)nødvendig i et demokratisk samfunn (..) for å forebygge uorden eller kriminalitet (..)».* Med dette menes, eksempelvis, at hvis politiet får informasjon om en forsyning med narkotika som skal komme over grensa fra Sverige, kan politiet stoppe den bilen det er snakk om på Svinesunds-grensa for å beslagelegge narkotikaen og pågripe personene i bilen. Politiet kan likevel ikke helgardere seg, med grunnlag i kriminalitetsbekjempelsen og nødvendighetskravet, og stoppe *alle* biler som kommer inn i Norge fra Sverige på *alle* grenseoverganger i *hele* landet. Et slikt eksempel vil overgå nødvendighetskravet da det på langt nær er «nødvendig» å stoppe alle for å ta èn. Henvisningen til «et demokratisk

66 Ref. Figuren over politiets virksomhet i kapittel 2.1

67 Justis- og beredskapsdepartementet, "popplyl." § 2 nr.8 og § 9

68 Justis- og beredskapsdepartementet, "Politiregisterloven." §5

69 Ref. Formålsparagrafen ovenfor

70 Justis- og beredskapsdepartementet, "mrl emkn." Artikkel 8 nummer 2

samfunn» speiler tilbake på befolkningens rett til privatliv og rett til å ikke bli overvåket av myndighetene. Det må videre være nødvendig å gjennomføre et spesifikt tiltak for å kunne oppfylle formålet med innsamlingen av opplysninger.

Til sist må opplysninger som innsamles og behandles etter politiregisterloven i utgangspunktet ha relevans. Med dette menes at opplysningene må være relevante til det formålet de er innsamlet og nødvendige for å oppfylle formålet med behandlingen. Hensikten med et krav til relevans er at politiet ikke skal ha anledning til å behandle eller samle inn opplysninger som er «kjekt å ha». Hvis formålet med behandlingen av opplysningene kan oppfylles med færre eller mindre sensitive opplysninger skal politiet gjøre dette[71]. Politiet og påtalemyndigheten kan dog likevel behandle opplysninger uten å ta hensyn til formål, nødvendighet eller relevans i en periode på inntil fire måneder med bakgrunn i Pool-ordningen.

De tre personvernprinsippene som fravikes i Pool-ordningen står helt sentralt i det som anses som godt personvern. Formålsbestemthet, nødvendighetskravet og kravet til relevans er grunnsteiner i både nasjonal- og internasjonal personvernlovgivning når det kommer til behandling av personopplysninger.

2.3.2 Informasjonssikkerhet/sporbarhet

Det andre kjernepunktet jeg skal ta for meg i denne oppgaven er informasjonssikkerhet/sporbarhet. Politiregisterlovens kapittel 4 regulerer informasjonssikkerhet og internkontroll, og er i stor grad utformet likt som tilsvarende kapittel om informasjonssikkerhet og internkontroll i Personopplysningsloven. Unntaket er kravet til sporbarhet etter § 17[72] og en noe utvidet bestemmelse om databehandlers rådighet over personopplysningene etter § 18[73].

Kravet til sporbarhet er en teknisk løsning for å kunne spore bruk av opplysninger, da særlig knyttet mot politiregistrene. Sporbarhet kan brukes til å administrere systemet, avdekke brudd på sikkerheten i systemet, samt avdekke og sanksjonere urettmessig behandling av personopplysninger. Dette er et internkontrollteknisk tiltak som hovedsaklig skal ivareta sikkerheten og forhindre urettmessig bruk av registrene. Likeledes er tiltaket ment som hjelp til å oppdage og håndtere brudd på sikkerheten[74].

I Politiregisterloven er informasjonssikkerhet i liten grad detaljregulert. Informasjonssikkerhet er derimot relativt detaljregulert i forskriften[75] til Politiregisterloven. Det er opp til den

[71] Justis- og politidepartementet, JD, "NOU 2003:21." Kapittel 13.5.3.1

[72] Justis- og beredskapsdepartementet, "Politiregisterloven." § 17

[73] Justis- og beredskapsdepartementet. §18

[74] "St.prp. Nr. 95 (2008-2009) – Regjeringen.no." Artikkel 22

[75] Justis- og beredskapsdepartementet, "Politiregisterforskriften." Kapittel 40

behandlingsansvarlige å etablere internkontrollrutiner og besørge god informasjonssikkerhet i sin organisasjon. Hvordan dette gjøres, eller med hvilke hjelpemidler, er regulert i forskrift. Det eneste som kreves i lovene er at det skal foreligge internkontroll- og informasjonssikkerhetsrutiner, at disse er planlagte og dokumenterte og at dokumentasjonen er tilgjengelig for de ansatte i organisasjonen og tilsynsmyndighetene. Datatilsynet, som tilsynsmyndighet, har produsert en veileder[76] for etablering av internkontroll for virksomheter som behandler personopplysninger. Direktoratet for Forvaltning og IKT (Difi) har på sin side laget en nettside[77] som inneholder veiledningsmateriell innen informasjonssikkerhet. I korte trekk handler informasjonssikkerhet om å sikre at informasjon;

- ikke blir kjent for uvedkommende (konfidensialitet)
- ikke blir endret utilsiktet eller av uvedkommende (integritet)
- er tilgjengelig ved behov (tilgjengelighet)

Etter Politiregisterlovens § 18 pålegges databehandlere tilsvarende taushetsplikt[78] som en som er ansatt i eller utfører tjeneste eller arbeid for politiet eller påtalemyndigheten. Videre kan enhver som er ansatt eller utfører arbeid eller tjeneste for databehandler kreves for politiattest, sannsynligvis for å kunne opprettholde taushetplikten og internkontrollen. Dette gjenspeiler også det faktum at opplysningene som politiet og påtalemyndigheten behandler er av en sensitiv art og må beskyttes i alle ledd.

Politiregisterlovens kapittel 5 regulerer utlevering og tilgang til opplysninger, hvor særlig § 20 om utlevering av ikke-verifiserte opplysninger inngår i denne oppgaven da dette speiler tilbake på pool-ordningen fra § 8, som omtalt ovenfor.

I likhet med bestemmelsene om vandelskontroll og politiattest er bestemmelser om taushetsplikt valgt samlet i ett lovverk. Bestemmelser knyttet til taushetsplikten er regulert i Politiregisterlovens kapittel 6[79]. Taushetspliktens omfang er gitt i § 23[80] . Den som arbeider i eller for politiet eller påtalemyndigheten har taushetsplikt når det kommer til opplysninger som vedkommende har fått kjennskap eller adgang til i kraft av sitt arbeid eller virke. Dette gjelder både for opplysninger knyttet til enkeltpersoner (en fysisk person) og opplysninger knyttet til bedrifter og bedriftshemmeligheter (juridiske personer). Det samme gjelder for opplysninger som dreier seg om en etterforskning eller lignende. Taushetsplikten gjelder også etter at ved-

[76] Datatilsynet, "Internkontroll."

[77] Difi, "Internkontroll i praksis - informasjonssikkerhet."

[78] Justis- og beredskapsdepartementet, "Lovvedtak 38 (2009-2010)." § 23 og § 35

[79] Justis- og beredskapsdepartementet, "Politiregisterloven." Kapittel 6

[80] Justis- og beredskapsdepartementet. § 23

kommende har avsluttet sitt arbeidsforhold i politiet eller påtalemyndigheten, slik at det ikke er anledning til å benytte opplysninger som vedkommende er kjent med i eget eller andres arbeid.

Taushetsplikten gjelder særlig i de tilfeller hvor opplysninger skal utleveres til andre enn politiet eller påtalemyndigheten. Innad i politiet og påtalemyndigheten er det lagt opp til en relativt fri flyt av opplysninger, sålenge det foreligger saklig eller tjenestlig behov hos den som mottar opplysningene, uavhengig av hvilket formål opplysningene opprinnelig var innsamlet til[81]. Politiet og påtalemyndigheten skal likevel, på generell basis, sørge for at opplysninger ikke blir gjort tilgjengelig eller kjent for uvedkommende. Dette innebærer i praksis både en aktiv og en passiv tilnærming til taushetsplikten. Dette kan gjøres gjennom fysiske hindre som gjør at uvedkommende ikke kan få tilgang til områder hvor opplysningene befinner seg eller lagres. Videre må den som har kjennskap til de taushetsbelagte opplysningene holde disse opplysningene for seg selv og ikke dele dem med uvedkommende.

2.3.3 Vandelskontroll og politiattester

I politiregisterlovens kapittel 7 reguleres vandelskontroll og attester. Dette er et viktig kjernepunkt da vandelskontroller og attester inneholder personopplysninger, ofte sensitive som sådan. Begrepet vandelskontroll omfatter utstedelse av politiattest, skikkethetsvurdering, vandelsvurdering, akkreditering og straffattest[82]. Siden vandelskontroll er en paraplybeskrivelse på *«bruk av opplysninger for å vurdere om en fysisk eller juridisk person er egnet til en bestemt stilling, virksomhet, aktivitet eller annen funksjon[83]»* må det differensieres i hvilke tilfeller den ene typen vandelskontroll, eksempelvis skikkethetsvurdering, fremfor den andre, eksempelvis politiattest skal brukes. I det følgende vil jeg gjøre kort rede for de ulike typene vandelskontroll og beskrive hvilke formål den enkelte vandelskontroll kan brukes til.

Akkreditering; «*Behandling av opplysninger i forbindelse med akkreditering av person kan foretas når vedkommende skal gis adgang til bestemte områder hvor det av sikkerhetsmessige eller tungtveiende ordensmessige grunner er nødvendig med en kontroll av personen, eller hvor det av samme grunner er nødvendig med en begrensning i antallet personer som skal ha tilgang til et sted[84].»*

---

81 Justis- og politidepartementet, JD, "NOU 2003:21." Kapittel 11.1, andre avsnitt

82 Justis- og politidepartementet, JD. Kapittel 15.1, første avsnitt. Jmf. Politiregisterloven § 2 nr.12

83 Justis- og beredskapsdepartementet, "Politiregisterloven." §2 nr.12

84 Justis- og beredskapsdepartementet, "Politiregisterforskriften." § 38-5, første avsnitt

Bruk av akkreditering blir oftest aktuelt når det skal foregå viktige statsbesøk, store idrettsarrangementer[85] eller andre store tilstelninger[86]. I slike tilfeller skal personer[87] som skal ha tilgang til områder med styrket sikkerhet være akkreditert, altså vurdert av Politiet/Politiets Sikkerhetstjeneste i forkant. Reguleringen av akkrediteringsinstituttet er lagt i Politiregisterforskriften[88].

Straffattest; «*Til bruk i den enkelte straffesak kan politiet, påtalemyndigheten, kriminalomsorgen og domstolene fremsette begjæring om straffattest om navngitt person.*
I straffattesten skal alle straffer, andre strafferettslige reaksjoner og andre tiltak som følge av lovbrudd anmerkes[89].»

En straffattest er således en oppsummering av en persons straffer og bøter, og brukes i strafferettspleien i forbindelse med straffesaker.

Skikkethetsvurdering; En skikkethetsvurdering går ut på å sammenstille opplysninger som politiet innehar for å vurdere *«om en person er skikket eller egnet for en stilling, funksjon, tillatelse, oppgave eller lignende[90].»*

En skikkethetsvurdering skiller seg fra en politiattest i den retning at en politiattest inneholder opplysninger som har bakgrunn i straffbare handlinger, mens en skikkethetsvurdering kan inneholde opplysninger som ikke er verifiserte eller basert på straffbare handlinger. Som navnet tilsier skal en skikkethetsvurdering gi et bilde på om en person er egnet til å inneha en stilling eller en tillatelse. I noen tilfeller har politiet opplysninger om en person som ikke er knyttet til straffbare forhold, eksempelvis at en person er særlig drikkfeldig. Denne personen må ikke ha gjort noe kriminelt i tilknytning til sin drikkfeldighet, men politiet har likevel registrert dette om vedkommende. Skulle han da søke om skjenketillatelse i forbindelse med sin restaurantvirksomhet, ville nok politiet kunne bruke informasjon om at han er særlig drikkfeldig og således sørge for at han ikke får skjenkeløyve. I andre tilfeller kan en persons tilhørighet til belastede miljøer ha betydning for om vedkommende er skikket til en viss type

85 Eksempelvis Olympiske Leker, Verdensmesterskap i fotball mv.

86 Eksempelvis utdeling av Nobelprisen, utdeling av Den Kongelige Norske St.Olavs Orden eller lignende

87 Som oftest gjelder dette journalister, fotografer eller lignende som skal dekke begivenheten og som er tilstede i kraft av sitt virke som journalist mv.

88 Justis- og beredskapsdepartementet, "Politiregisterforskriften." §38-5

89 Justis- og beredskapsdepartementet, "Politiregisterloven." § 46

90 Justis- og politidepartementet, JD, "NOU 2003:21." Kapittel 15.13.7, første avsnitt

stilling. Det samme kan gjelde personer som flere ganger er anmeldt for seksuelle overgrep, men aldri straffet for det. Slike type opplysninger, som enten er overskuddsinformasjon eller som sier noe om en persons karakter, må anføres i vurderingen at de er nettopp det – ikke--verifisert informasjon.

Vandelsvurdering; En vandelsvurdering er en vurdering som skjer uten at den vurderingen gjelder vet at vurderingen blir gjort. Hensikten med en vandelsvurdering er *«å kontrollere en persons tidligere vandel før han pålegges å utføre en lovbestemt plikt.*[91]*».*

En vandelsvurdering brukes til særlige spesifikke formål, og ifølge Politiregisterutvalget finnes det bare to tilfeller hvor vandelsvurdering blir brukt. Dette er i forbindelse med *«valg og uttaking av meddommere og lagrettemedlemmer og til bruk for militær tjeneste»*[92]*.*

Politiattest (ordinær, uttømmende og begrenset); Utgangspunktet for en ordinær politiattest er en redegjørelse av *«hvorvidt en person har vært gjenstand for strafferettslige reaksjoner eller for andre tiltak i anledning straffbare handlinger som han har begått*[93]*».*

Den ordinære politiattesten har flere unntak og begrensninger på hva som skal oppføres i den. Disse begrensningene og unntakene stipuleres i Politiregisterloven[94] § 40.

En uttømmende politiattest medfører at alt politiet har registrert gjennom SSP[9596] skal påføres en attest. I motsetning til ordinær politiattest har en uttømmende politiattest ingen begrensninger bakover i tid[97]. Det rettslige grunnlaget for utstedelse av en uttømmende politiattest må fremgå av særlovgivning, eksempelvis for opptak til Politihøgskolen[98].

En begrenset politiattest skal kun anmerke spesifikke lovbestemmelser som er brutt. I likhet med uttømmende politiattest fremgår det rettslige grunnlaget for bruk av begrenset politiattest gjennom særlovgivning. Gjennom den enkelte særlovgivning forstås det implisitt hvorvidt begrenset politiattest skal benyttes, da hvert enkelt straffebud som skal påføres attesten er redegjort for i paragrafen. Et eksempel på dette er Fjellova §25, tredje ledd; «*Fjellstyret kan nekte*

91 Justis- og politidepartementet, JD. Kapittel 15.14, første avsnitt

92 Justis- og politidepartementet, JD. Kapittel 15.2.2, femte avsnitt

93 Justis- og politidepartementet, JD. Kapittel 4.20.4, første avsnitt

94 Justis- og beredskapsdepartementet, "Politiregisterloven." § 40

95 Justis- og politidepartementet, JD, "NOU 2003:21." Kapittel 4.6, Det Sentrale Straffe- og Politiopplysningsregister

96 Justis- og beredskapsdepartementet, "Politiregisterforskriften." Kapittel 49

97 Justis- og politidepartementet, JD, "NOU 2003:21." Kapittel 4.20.4, andre avsnitt

98 Justis- og beredskapsdepartementet, "politil." § 24b, første ledd, tredje setning

å skrive ut jaktkort til den som i dei 3 siste åra rettskraftig er dømd til straff, eller har vedteke førelegg om straff, for brot mot nokor føresegn om jakt[99]*.»* Altså kan Fjellstyret nekte å skrive ut jaktkort til noen som har brutt paragrafer i tilknytning til jakt. I et slikt tilfelle må politiet utstede en begrenset politiattest som opplyser om hvorvidt vedkommende er dømt eller straffet for brudd på lovgivning eller bestemmelser som omhandler jakt.

2.3.4 Informasjonsplikt, retting, sperring og sletting

I kapittel 8 reguleres informasjonsplikt, innsyn, retting, sperring og sletting. Informasjonsplikten og innsynsretten er ment å ivareta den registrertes interesser og dens mulighet til å føre kontroll med de opplysninger som politiet behandler om den registrerte. Informasjonsplikten på sin side omhandler den behandlingsansvarliges plikt til å informere den registrerte om navn og adresse på den behandlingsansvarlige, formålet med behandlingen, om opplysningene vil bli utlevert og eventuelt til hvem, at det er frivillig å gi fra seg opplysningene og eventuell annen informasjon som er relevant for den registrerte i forbindelse med behandlingen[100]. I forhold til politiet og påtalemyndigheten som behandlingansvarlig er de i stor grad unntatt informasjonsplikten etter personopplysningsloven § 23 bokstav b[101], med hensyn til kriminalitetsbekjempelsen. Det samme unntaket omtales i Politiregisterloven[102]. For Politiet og påtalemyndigheten gjelder informasjonsplikten i de tilfeller hvor opplysninger utleveres til andre offentlige etater eller private i den registrertes interesse[103], med visse unntak[104].

Innsynsretten er den registrertes rett til å vite hvilke opplysninger som behandles om vedkommende og kunne kontrollere om opplysningene som behandles er korrekte. I Politiregisterloven er innsynsretten betydelig begrenset sammenlignet med Personopplysningslovens § 18[105]. Politiregisterloven skiller mellom innsyn i straffesak og utenfor straffesak. I straffesak er det straffeprosessloven[106] som regulerer partsinnsyn. Utenfor den enkelte straffesak er det Politiregisterloven som regulerer innsyn. Som hovedregel har den registrerte rett til å vite hva som er registrert om seg[107], med mindre unntakene[108] gjør seg gjeldende. Når det

[99] Landbruks- og Matdepartementet, "fjell." § 25, tredje ledd

[100] Justis- og beredskapsdepartementet, "popplyl." § 19

[101] Justis- og beredskapsdepartementet. § 23 bokstav b

[102] Justis- og beredskapsdepartementet, "Politiregisterloven." § 48 nr.2

[103] Justis- og beredskapsdepartementet. § 48

[104] Justis- og beredskapsdepartementet. § 48 nr.1 tom. nr. 4

[105] Justis- og beredskapsdepartementet, "popplyl." § 18

[106] Justis- og beredskapsdepartementet, "Strpl." § 242 og § 242 bokstav a

[107] Justis- og beredskapsdepartementet, "Politiregisterloven." § 49

[108] Justis- og beredskapsdepartementet. § 49, fjerde ledd nr. 1 tom. nr 5

kommer til unntakene kan en særlig merke seg at retten til innsyn er unntatt i de tilfeller hvor formålet med behandlingen av opplysningene er kriminalitetsbekjempelse.
Videre reguleres bestemmelser om retting, sperring og sletting. Politiregisterutvalget gjør rede for disse begrepene i sin utredning[109] som det følgende;
Retting; *Når ufullstendige eller ukorrekte opplysninger suppleres med opplysninger som gjør dem korrekte.*
Sperring; *Når opplysninger gjøres midlertidig utilgjengelig for politietaten, og spesielle tilfeller kan føre til at de blir gjort tilgjengelig igjen.*
Sletting; *Når opplysninger irreversibelt fjernes, slettes for alltid.*
Reglene om retting, sperring og sletting er viktige på flere måter. For det første bidrar reglene til at den behandlingsansvarlige har et bevisst forhold til opplysningskvalitet. For det andre bidrar reglene til ivaretakelse av den registrertes personvern og rettssikkerhet. Til slutt kan de bidra som en kontrollfunksjon på den behandlingsansvarlige slik at det ikke foregår behandling av opplysninger som burde vært slettet eller sperret, eller som har tjent sitt formål og skal slettes deretter.

I Politiregisterlovens kapittel 9 til 11 omtales blant annet adgangen til klage, bestemmelser om tilsynsmyndigheter samt særbestemmelser for Politiets Sikkerhetstjeneste (PST).
De resterende kapitlene er standardkapitler om forskrifter og sluttbestemmelser.
Jeg velger å ikke vie disse kapitlene særlig oppmerksomhet da de i liten grad nevnes i mine drøftinger og har således begrenset relevans opp mot kjernepunktene og oppgavens problemstillinger.

[109] Justis- og politidepartementet, JD, "NOU 2003:21." Kapittel 17

3 Teori

I dette kapittelet vil jeg gjøre rede for og drøfte interesseteorien, som er teorigrunnlaget for mine videre analyser og vurderinger av høringssvarene til NOU 2003:21.

I kapittel 3.1 vil jeg gjøre kort rede for hva personvern er, hva som oppfattes som personvern i norsk kontekst og hvilke prinsipper som er ment å skape et godt personvern.

I kapittel 3.2 vil jeg gjøre nærmere rede for interesseteorien[110] presentert gjennom Schartum og Bygrave[111] og belyse hvordan denne er relevant for oppgaven videre. Med dette mener jeg å ha en eksplorerende tilnærming til interesseteorien – altså å fremstille den i sin helhet med bakgrunn i Schartum/Bygraves fremstilling, for så senere avgjøre hvilke deler av interesseteorien som gjør seg gjeldende for mine problemstillinger og vurderinger.

I kapittel 3.3 vil jeg presentere de delene av interesseteorien som jeg mener har empirisk relevans for de tre kjernepunktene jeg skal se nærmere på; Pool-ordningen, vandelskontroll og informasjonssikkerhet/sporbarhet.

3.1 Hva er personvern?

Personvern handler om den enkeltes rett til privatliv og en rett til å bestemme over egne personopplysninger. Retten til privatliv er forankret både i Den Europeiske Menneskerettighetskonvensjonen[112] og i Grunnloven[113]. I norsk forståelse av begrepet personvern omfattes også retten til å bestemme over egne personopplysninger og deres bruk og spredning. Et godt utviklet personvern ivaretar sentrale demokratiske prinsipper som deltakelse, den frie meningsdannelse og vernet om privatlivet og den private sfære.

Personvernet baserer seg på flere prinsipper som nærmere forklarer hva begrepet «personvern» inneholder. I all hovedsak skal personvernet være til for å verne om den enkeltes personlige integritet og rett til privatliv. I de tilfeller hvor personopplysninger må behandles skal en alltid tilstrebe at et minimum at personopplysninger brukes for å oppnå formålet med behandlingen. Det er også helt sentralt at behandling av personopplysninger har et rettslig grunnlag, være seg enten samtykke, nødvendighet eller lovhjemmel, og at behandlingen av personopplysningene har et bestemt formål. Selve opplysningene bør ha en så god kvalitet som mulig og være relevante for den behandlingen som skal foregå. Inkludert i personvernbegrepet ligger også den enkeltes rett til å føre kontroll med egne opplysninger. Denne retten ivaretas som oftest av innsynsretten og den klageadgang som foreligger hos de fleste som

[110] Selmer and Blekeli, *Data og personvern*.

[111] Schartum and Bygrave, *Personvern i informasjonssamfunnet*. Kapittel 2.4 s.44-87

[112] Justis- og beredskapsdepartementet, "mrl emkn." Artikkel 8

[113] Justis- og beredskapsdepartementet, "Grl." § 102

behandler personopplysninger. Den som behandler personopplysninger plikter også å sikre opplysningene mot uautorisert adgang, spredning eller offentliggjøring, sålenge det ikke foreligger samtykke fra den opplysningene angår.

3.1.1 Tre perspektiver på personvern

Schartum/Bygrave[114] beskriver i sin bok tre ulike perspektiver på personvern. Dette omfatter integritetsperspektivet, beslutningsperspektivet og maktperspektivet.

Integritetsperspektivet, også kjent som sfæreteori, er den mest tradisjonelle oppfatningen av hva som er personvern. Dette perspektivet beskriver at hver enkelt person har sine egne sfærer, altså deler av livet, som har *«forskjellig grad av intimitet eller sensitivitet for den enkelte»*[115]. Avhengig av hvor sensitiv den enkelte sfære er, må beskyttelsesbehovet for sfæren avpasses deretter. Forfatterne skjelner mellom seks ulike sfærer, eller ulike typer integritet; stedlig integritet, kroppslig integritet, psykisk integritet, kommunikasjonsintegritet, informasjonsintegritet og kontekstuell integritet.

Stedlig integritet omhandler respekt for andre menneskers private geografiske- eller fysiske områder. Med dette menes et territorium som er «fredet» fra andres forstyrrelser eller urettmessig inngripen.

Kroppslig integritet omhandler den enkeltes fysiske kropp. Nærmere bestemt handler kroppslig integritet om at den enkeltes fysiske legeme ikke skal krenkes av noen på en urettmessig måte. Eksempelvis kan innsamling av biologiske data være krenkende med tanke på personvernet og den kroppslige integriteten. Det samme kan gjelde for blodprøver, DNA-undersøkelser eller bruk av sporingsteknologi[116] m.v.

Psykisk integritet omhandler et vern av den enkeltes tanker og opplevelse av selv. Dette kan eksempelvis gjelde for personer som blir satt i en usikker livssituasjon pga uavklart statstilhørighet eller så enkelt som at noen leser andres dagbøker.

Kommunikasjonsintegritet omhandler den enkeltes rett til å kommunisere fritt med andre mennesker, uten at andre skal åpne våre brev, lytte på våre telefonsamtaler eller lese meldinger eller chat på andres mobiltelefoner.

Informasjonsintegritet handler om den enkeltes rett til å *«generere, bearbeide eller behandle informasjon*[117]*»* om seg selv, uten forstyrrelser fra andre. Dette gjelder uavhengig om informasjonen kommuniseres til andre eller ei.

---

[114] Schartum and Bygrave, *Personvern i informasjonssamfunnet*. Kapittel 2.2

[115] Schartum and Bygrave. Side 31

[116] Eksempelvis GPS-merking av demente personer eller bruk av fotlenker på straffedømte.

[117] Schartum and Bygrave, *Personvern i informasjonssamfunnet*. Side 32 fjerde avsnitt

Kontekstuell integritet omhandler den enkeltes rett til å vurdere om en type informasjon fremstår relevant eller aktuell i en gitt situasjon. Det faller seg åpenbart at banken må ha våre inntektsopplysninger når vi skal søke om huslån og at legen må ha informasjon om vår helsetilstand for å kunne gi den riktige behandlingen. Det forekommer likevel situasjoner hvor noen avkrever informasjon som ikke er relevant i den enkelte situasjon eller relasjon. Et eksempel på dette kan være prøvetimer ved treningssentre. I mange tilfeller avkreves den som ønsker å benytte seg av en prøvetime for unødvendig store mengder kontaktinformasjon. Dette er klart at ikke står i stil med «formålet» med prøvetimen, men treningssenteret er åpenbart interessert i å kunne kontakte vedkommende senere med gode tilbud, salg og reklame.

Beslutningsperspektivet tar utgangspunkt i at beslutninger ofte fattes på bakgrunn av personopplysninger. I dette perspektivet skal også personvernet ivaretas. I dette ligger det at opplysningene som danner grunnlaget for beslutningen ikke alltid er av god kvalitet eller relevans, og således kan personvernet være truet. Dess større eller mer omfattende en beslutning er, dess viktigere bør de aktuelle personvernspørsmålene være.

Maktperspektivet omhandler forholdet mellom maktutøveren (staten) og befolkningen. I dette perspektivet er det relasjonen mellom disse to som kan utløse personvernteoretiske spørsmål. Dette har særlig tilknytning til det vi omtaler som velferdssamfunnet, hvor statlige organer i mange tilfeller behandler opplysninger om den enkelte for å opprettholde velferdssamfunnet. Dette kommer særlig til syne når personopplysninger behandles av statlige organer ved hjelp av automatiserte løsninger, eller ved bruk av andre typer IKT-løsninger. Spørsmålet er om maktbalansen er god nok i den forstand at personvernet også ivaretas ved bruk av slike løsninger, eller som de statlige organene har for mye makt og at løsningene skaper en opplevelse av avmakt hos befolkningen. Maktperspektivet er ment å belyse denne relasjonen.

Når det kommer til Politiregisterloven er det særlig maktperspektivet og beslutningsperspektivet som kan sees som relevante. Politiet og påtalemyndigheten fatter ofte beslutninger på bakgrunn av personopplysninger. Disse beslutningene kan i mange tilfeller medføre alvorlige konsekvenser for den beslutningen gjelder, og personvernet må således ivaretas for å besørge at beslutningene fattes på riktig grunnlag. I tillegg er politiet og påtalemyndigheten en maktutøver ovenfor befolkningen. Med bakgrunn i Politiregisterloven bruker maktutøveren flere elektroniske registre og forskjellige IKT-løsninger for å kunne utøve sitt virke. Det er således

viktig at personvernet ivaretas når slike løsninger benyttes og at maktbalansen mellom maktutøveren og befolkningen ikke er skjev.

3.2 Interesseteorien

Interesseteorien slik den står idag er basert på flere forskjellige kilder. Utgangspunktet for interesseteorien er Blekeli/Selmer[118], mens Schartum/Bygrave[119] bearbeidet den videre og tok inn flere relevante kilder, blant annet Jon Bing[120] og Boe-utvalgets innstilling i NOU 1993:22[121]. I all hovedsak er interesseteorien en systematisering av Personopplysningslovens bestemmelser. Den er delt inn i fem interesser hvor hver av interessene har tilhørende krav. Disse kravene er et slags «dypdykk» inn i den enkelte interesse og gir et mer nyansert bilde av hva interessen omhandler. I stor grad kan både interessene og kravene fra interesseteorien gjenfinnes om man leser Personopplysningsloven og dens bestemmelser nøye.

Et sentralt aspekt ved personvernteori er at en søker å oppnå balanse mellom personvern og det som skal reguleres. Dette betyr ikke nødvendigvis at det alltid skal balanseres 50-50, men at det hele tiden må gjøres avveininger rundt hvilke type interesser som skal tillegges vekt i det enkelte tilfellet. Schartum/Bygrave beskriver nettopp dette på følgende måte;

« Avveiningen mellom personvern og andre mål er nesten aldri et spørsmål om enten-eller. Snarere handler diskusjonen om hvordan (..) kriminalitet kan bekjempes ***samtidig***[122] *som folks personvern (og rettssikkerhet) blir godt ivaretatt.*[123]*»*

Med dette mener Schartum og Bygrave at viktige samfunnsinteresser, som kriminalitetskjempelse, må finne sted. Samtidig må den enkeltes personvern være ivaretatt når kriminalitetsbekjempelsen skjer. Skulle en utelukkende tatt hensyn til alle personverninteresser og gitt befolkningen «totalt personvern» hadde bekjempelse av kriminalitet vært nærmest umulig. Målet må være en Ole Brum-filosofi – ja takk, begge deler.

118 Selmer and Blekeli, *Data og personvern*.

119 Schartum and Bygrave, *Personvern i informasjonssamfunnet*.

120 Bing, *Personvern i faresonen*.

121 Boe-utvalget, "NOU 1993:22."

122 Min utheving

123 Schartum and Bygrave, *Personvern i informasjonssamfunnet*. Side 47

Interesseteorien består av fem interesser[124];

1. Interessen i å bestemme over tilgangen til opplysninger om egen person
2. Interessen i innsyn og kunnskap
3. Interessen i opplysnings- og behandlingskvalitet
4. Interessen i forholdsmessig kontroll
5. Interessen i brukervennlig behandling

Hver av interessene er videre delt inn i krav som skal gi en dypere forståelse av hva hver enkelt interesse faktisk innebærer.

Til interessen i å bestemme over tilgangen til opplysninger om egen person er det tillagt fire krav;

1. Krav om etablert tillitsforhold
2. Krav om konfidensialitet
3. Krav om beskyttet privatliv
4. Krav om vern av individets identitetsbilde

Til interessen i innsyn og kunnskap er det tillagt fire krav;

1. Krav om rettsinformasjon
2. Krav om generelt innsyn
3. Krav om individuelt innsyn
4. Krav om begrunnelse

Til interessen i opplysnings- og behandlingskvalitet er det tillagt to krav;

1. Krav om opplysningskvalitet
2. Krav om behandlingskvalitet

Til interessen i forholdsmessig kontroll er det tillagt fire krav;

1. Kravet om forholdsmessighet mellom veiledning og kontroll
2. Kravet om forholdsmessighet mellom forhåndskontroll og etterkontroll
3. Kravet om forholdsmessighet mellom kontroll til de registrertes gunst og til deres ugunst
4. Kravet om forholdsmessighet mellom ekstern- og intern kontroll

Til interessen i brukervennlig behandling er det tillagt fire krav;

1. Krav om lydhørhet
2. Krav om forståelighet
3. Krav om uhindret dialog

[124] Schartum and Bygrave. Kapittel 2.4

4. Krav om driftsstabilitet

I det følgende vil jeg gjøre rede for hver enkelt interesse med tilhørende krav. Jeg vil hovedsaklig fokusere på de delene av interesseteorien jeg mener er relevante i denne oppgaven. Jeg vil også spesifisere hvilke deler av interesseteorien jeg vil anvende når jeg analyserer høringsinstansenes svar til NOU 2003:21. Dette gjør jeg i kapittel 3.3.

3.2.1 Interessen i å bestemme over tilgangen til opplysninger om egen person

En omtaler ofte et slags eierskap eller råderett når det kommer til opplysninger om egen person, og dette er delvis både korrekt og ukorrekt på samme tid. Et eierskap eller råderett knyttet til det å eie en gjenstand eller en eiendom lar seg bare til dels sammenligne med det eierskap eller råderett som vises til når det kommer til personvern. Med dette menes at et eierskap eller råderett over en eiendom eller gjenstand strekker seg et godt stykke lengre enn hva eierskap eller råderett til personopplysninger gjør. Skulle man hatt den samme råderett over sine personopplysninger som man har sin eiendom, ville store deler av samfunnet vært tilnærmet ubrukelig. Hver eneste dag må vi gi fra oss personopplysninger for å kunne være en del av et moderne, demokratisk samfunn. Vi bruker mobiltelefonene våre nærmest kontinuerlig som avgir GPS-posisjoner og aktivitetsdata, vi kjøper gjenstander og tjenester med «digitale penger» som etterlater seg digitale fotspor, vi får akutt helsehjelp, vi søker arbeid og betaler vår skatt. I alle disse tilfellene, som er en del av vårt daglige liv, avgir vi personopplysninger. Hvis råderetten over personopplysninger da skulle vært lik som råderetten over eiendom ville de fleste av disse tjenestene eller dagligdagse gjøremål være umulig å gjennomføre. En kan ikke leve i et moderne og demokratisk samfunn og forvente full anonymitet og totalt personvern. Det er heller slik at personvernet, som prinsipp, må understøtte disse tjenestene og dagligdagse gjøremål og bidra til at den enkelte ikke får sitt privatliv eller sin identitet krenket. Det finnes utallige eksempler på at vårt eierskap eller råderett over opplysninger om egen person er begrenset, men for å knytte dette til oppgaven er kriminalitetsbekjempelsen et godt eksempel. I de fleste, om ikke alle, tilfeller av kriminalitetsbekjempelse ville en selvråderett over personopplysninger være nokså utenkelig. Hvis hver enkelt av de som begår kriminalitet skulle råde fullt og helt over sine personopplysninger ville bekjempelsen av den vært umulig. Da ville den kriminelle få vite at han eller hun er i politiets søkelys, hvilke opplysninger politiet innehar og i utgangspunktet kunne han eller hun nekte at politiet behandlet opplysninger om vedkommende. Slik er det altså ikke. Det demokratiske samfunnet gir styresmaktene et ansvar i å, eksempelvis, sørge for at kriminalitet reduseres eller bekjempes. For å oppnå

dette må personopplysninger samles inn og behandles uten at den som «eier» opplysningene kjenner til det. Til dette har vi lovverk som ivaretar samfunnsinteressen i å bekjempe kriminalitet.

3.2.1.1 Kravet om etablert tillitsforhold

For å kunne akseptere at myndighetene behandler opplysninger om personer uten deres samtykke eller viten må det finnes en grunnleggende tillit til myndighetene eller de som behandler opplysningene våre. Kravet om et etablert tillitsforhold er like viktig i de tilfellene hvor behandlingen av personopplysninger baserer seg på et informert samtykke[125], som det er i de tilfellene hvor lovhjemmel eller nødvendighet er det rettslige grunnlaget for behandlingen. Kravet om et etablert tillitsforhold tilfaller i hovedsak den behandlingsansvarlige. Det er den behandlingsansvarliges plikt å etterleve lovverket som regulerer behandlingen og det er dens plikt å anerkjenne den registrerte som en person som har rett til sin mening og en respektfull behandling. I dette omfattes også en plikt hos den behandlingsansvarlige til å informere den registrerte om hvordan behandlingen foregår og hvilke regler som gjelder for behandlingen av personopplysninger. En slik type åpenhet skal sørge for at den registrerte har tillit til at hans eller hennes personopplysninger behandles i tråd med lovgivningen, at uvedkommende ikke får tilgang til opplysningene som behandles og at et vedtak som fattes er fattet på et så riktig grunnlag som mulig.

3.2.1.2 Krav om konfidensialitet

Videre er et krav om konfidensialitet sentralt. Konfidensialitet skal sørge for at personopplysninger ikke tilkommer uvedkommende og at en eventuell spredning av personopplysninger gjøres i et omfang som den registrerte selv kan akseptere eller tillate. I mange tilfeller behandles personopplysninger med samtykke som rettslig grunnlag. Samtykket setter også krav til graden av konfidensialitet og dermed i hvilken grad opplysningene skal gjøres kjent for andre eller spres. Kravet om konfidensialitet ivaretas hovedsaklig av en relativt veletablert institusjon i forvaltningen – taushetsplikten. Både den aktive- og den passive delen av taushetsplikten er ment å ivareta kravet om konfidensialitet.

Med hensyn til kriminalitetsbekjempelsen fremstår konfidensialitet som særlig viktig, da den skal ivareta to sider – den behandlingsansvarliges interesser og den registrertes interesser. Den behandlingsansvarliges interesser omhandler et mål om å bekjempe kriminalitet og hindre at den opplysningene gjelder får mulighet til å tilpasse sin atferd eller forklaring i en retning som kan hindre kriminalitetsbekjempelsen. På den andre siden må den registrerte, den opplysnin-

[125] Justis- og beredskapsdepartementet, "popplyl." §2 nr.7

gene gjelder, ha et visst vern knyttet til sine opplysninger. Med dette menes at den registrertes opplysninger ikke skal tilkomme uvedkommende da opplysninger om kriminelle forhold i mange tilfeller kan ha negative ringvirkninger for den registrerte hvis opplysningene blir kjent for uvedkommende. En kan se for seg at opplysninger som politiet eller påtalemyndigheten innehar kan komme uvedkommende for øre og denne uvedkommende kan ønske å påføre den registrerte en form for skade eller represalie.

3.2.1.3 Krav om beskyttet privatliv

I tett sammenheng med kravet til konfidensialitet finner vi kravet om beskyttet privatliv. Selv om disse to kravene har noe overlapp omhandler kravet om et beskyttet privatliv mer enn vern om opplysninger om den enkelte eller den registrerte. Kravet om et beskyttet privatliv er ment å beskytte eksempelvis en husstand eller noens privatliv. I forhold til kriminalitetsbekjempelsen må kravet om et beskyttet privatliv sees som et slags «ettervern», altså at en som har begått en kriminell handling skal kunne leve et tilnærmet normalt liv i etterkant av at saken er avgjort. I dette ligger det et vern om å få sitt privatliv «hengt ut» i offentligheten, sitt bosted offentliggjort eller sine familiære forhold gjort kjent for alle og enhver. Det er likevel noe uklart hvor langt dette kravet strekker seg, men eksempelvis er det per idag ikke gitt tillatelse til å gjøre offentlig kjent hvor pedofilidømte har bosted, både i frykt for represalier og offentlig sjikane.

3.2.1.4 Krav om vern av individets identitetsbilde

I noen sammenheng med kravet om et beskyttet privatliv kommer kravet om vern av individets identitetsbilde. Et vern om individets identitetsbilde omhandler en rett til å ikke få vite opplysninger om en selv som kan fremstå opprivende eller forstyrrende for den opplysningene gjelder. Eksempelvis forekommer det tilfeller hvor personer ikke vet at de er adopterte eller at de har vært ivaretatt av en barnevernsinstitusjon i barndommen. Slike opplysninger kan virke opprivende og forstyrrende for den de angår, og de har således rett til å *ikke vite* slike opplysninger. Den enkeltes identitetsbilde, altså opplevelse av selv og eget liv, skal vernes.

3.2.2 Interessen i innsyn og kunnskap

En av de aller mest grunnleggende personverninteressene er interessen i innsyn og kunnskap. Denne interessen er ment å ivareta den registrertes mulighet til å gjøre seg kjent med opplysninger som omhandler ham eller henne, hvordan disse opplysningene behandles, om opplysningene som behandles er korrekte og oppdaterte og om den behandlingsansvarlige behandler opplysninger om vedkommende i tråd med lovverket. For at den registrerte skal kunne ivareta sine rettigheter og plikter må de også ha kunnskap om behandling av personopplysninger.

Med hensyn til kriminalitetsbekjempelsen er interessen i innsyn og kunnskap noe redusert, da det i mange tilfeller foreligger en sterkt begrenset innsynsrett og store deler av politiets og påtalemyndighetens virksomhet er underlagt sterk konfidensialitet og taushetsplikt. I det følgende vil jeg gjøre rede for de fire krav som ligger til interessen i innsyn og kunnskap, og forsøke å koble kravene opp mot kriminalitetsbekjempelsen.

3.2.2.1 Kravet om rettsinformasjon

Det første kravet under interessen i innsyn og kunnskap er kravet om rettsinformasjon. Kravet omtaler hvilke lover, regler, forskrifter mv. som gjelder for behandling av personopplysninger og i hvilken grad den registrerte har adgang til disse. For at den registrerte skal kunne oppfylle sine plikter og rettigheter når det behandles personopplysninger må også lovverket som regulerer behandlingen være tilgjengelig slik at den registrerte vet hva som er gjeldende rett. Inkludert i dette kravet ligger også et krav om veiledningsplikt hos den behandlingsansvarlige – altså at den registrerte skal kunne få forklart hvordan gjeldende regelverk gjør seg aktuelt for den enkeltes situasjon. På den andre siden er det også viktig at kravet om rettsinformasjon følges av den behandlingsansvarlige. Tilfeller av begrenset kunnskap rundt gjeldende lovverk hos den behandlingsansvarlige kan medføre negative konsekvenser for den registrerte og dens personvern. I lys av kriminalitetsbekjempelsen baserer kravet om rettsinformasjon seg hovedsaklig på publisert lovverk, gjerne gjennom Lovdata-stiftelsen.

3.2.2.2 Kravet om generelt innsyn

Kravet om generelt innsyn omtaler en rett til å få informasjon om hvordan personopplysninger behandles på et generelt grunnlag uten at det nødvendigvis må være koblet til en fysisk person. Ved bruk av generelt innsyn kan befolkningen få rede på hvordan personopplysninger behandles, hva opplysningene genererer av informasjon og hvordan opplysningene brukes videre og på denne måten lettere kunne ivareta sitt eget personvern i forkant av en behandling. Som en hovedregel kan innsynsbegjæringer avvises med hensyn til kriminalitetsbekjempelsen[126]. En må således anta at et krav om generelt innsyn i noen grad kan være begrenset med hensyn til kriminalitetsbekjempelsen, rikets sikkerhet eller lignende. En inngående utredning på hvordan politiet og påtalemyndigheten behandler personopplysninger og hva som genereres ut av dem kan få uheldige konsekvenser, og en må anta at Personopplysningslovens[127] § 18 blir ledesnoren for hva politiet kan opplyse i forbindelse med et krav om generelt innsyn.

[126] Justis- og beredskapsdepartementet, "Politiregisterloven." § 49, fjerde ledd

[127] Justis- og beredskapsdepartementet, "popplyl." §18, bokstav a) til f)

3.2.2.3 Kravet om individuelt innsyn

Kravet om individuelt innsyn er, i motsetning til generelt innsyn, knyttet til opplysninger om en bestemt person. Dette kravet er særlig viktig for ivaretakelsen av den enkeltes personvern, da den registrerte har rett til å vite hvilke opplysninger som er registrert om ham eller henne. På denne måten kan den registrerte føre kontroll med sine egne opplysninger, hva de brukes til og kontrollere i hvilken grad opplysningene gjenspeiler virkeligheten. Man kan vanligvis ikke be om innsyn i opplysninger som angår noen annen enn seg selv. Kravet om individuelt innsyn ivaretar også muligheten for å vurdere om et etablert tillitsforhold[128] er tilstede. Når det kommer til politi- og påtalemyndighetens behandling av opplysninger kan man be om individuelt innsyn, og få vite hva som er registrert av opplysninger om en. Det er likevel gjort unntak hvis opplysningene brukes i kriminalitetsbekjempende virksomhet, dette for å forhindre at den registrerte tilpasser sin atferd eller forklaring ovenfor politiet eller påtalemyndigheten og dermed kan forringe kriminalitetsbekjempelsen.

3.2.2.4 Kravet om begrunnelse

Det siste kravet innenfor interessen i innsyn og kunnskap er kravet om begrunnelse. Dette er et krav som oftest kommer til syne etter at personopplysningene har blitt behandlet og det er fattet et vedtak. Et vedtak som er fattet kan i seg selv generere nye personopplysninger og som registrert kan man be om begrunnelse for vedtaket. Dette har til hensikt å sikre at vedtaket er fattet på bakgrunn av korrekte og oppdaterte opplysninger. Dette er også med på å sikre at den behandlingsansvarlige gjennomfører sitt arbeid i tråd med lovverket og et krav om begrunnelse kan også gi bekreftelse eller avkreftelse på hvorvidt den behandlingsansvarlige har hjemmelsgrunnlag for å behandle personopplysninger. I de tilfeller hvor vedtak fattes av en datamaskin må et krav om begrunnelse si noe om hvordan datamaskinprogrammet fungerer og hvordan programmet behandler opplysninger og fatter vedtak.

3.2.3 Interessen i opplysnings- og behandlingskvalitet

Interessen i opplysnings- og behandlingskvalitet er en viktig interesse, kanskje særlig innen kriminalitetsbekjempelsen. Med opplysningskvalitet mener man i hvilken grad opplysningene egner seg til å gjengi et bilde av det de er ment å representere. Med behandlingskvalitet menes hviken kvalitet systemene og rutinene som er satt til å behandle opplysningene har.

[128] Ref. Kravet om etablert tillitsforhold i interessen i å bestemme over tilgangen til opplysninger om egen person

3.2.3.1 Krav om opplysningskvalitet

Kravet til opplysningskvalitet er det første av to krav i interessen i opplysnings- og behandlingskvalitet. Interesseteorien deler kravet til opplysningskvalitet i to deler; «forholdet mellom opplysningene og det de er ment å representere eller gjengi» og «forholdet mellom opplysninger og opplysningenes videre bruksformål[129]». Den første delen omhandler opplysningenes presisjonsnivå, opplysningenes fullstendighet og opplysningenes riktighet. Kort sagt gir denne spesifiseringen en oversikt over hvor godt opplysningene passer til det de skal gjengi; hvor detaljert blir personen beskrevet, om alle opplysningene som trengs for å beskrive personen er tatt med og om opplysningene er korrekte.

For å kunne bekjempe kriminalitet er politiet i stor grad avhengig av opplysninger, og opplysningenes kvalitet er ikke alltid avklart eller av beste sort. Opplysningene som benyttes kan være basert på tips fra publikum som har tilkommet politiet og de kan være basert på politiets egne observasjoner eller etterforskningssteg. Politiet, eller den som behandler opplysninger, skal til enhver tid tilstrebe at opplysningene har en så god kvalitet som mulig. Skulle opplysningene ha en dårlig kvalitet kan dette få følger for kriminalitetsbekjempelsen, enten ved at kriminalitetsbekjempelsen blir vanskeliggjort eller umulig, til at uriktig person blir anklaget for noe han eller hun ikke har gjort. Dette kan sees som ytterpunktene av følgene for dårlig opplysningskvalitet, men det viser likevel viktigheten av god opplysningskvalitet.

Den andre delen omtaler hvorvidt opplysningene som er tilstede fyller et formål. Med dette menes om «det foreligger en logisk sammenheng mellom opplysningene og vedkommende bruksformål», om «det er rettslig adgang til å benytte opplysningene til vedkommende formål», og om «opplysningene virker troverdige»[130]. I en viss grad er denne delen preget av skjønn, altså er det vanligvis personer som må vurdere om opplysningene er relevant for det formålet de skal brukes og om det foreligger rettslig grunnlag for å behandle opplysningene. En slik vurdering av relevans er neppe enkel og det kan nok være fristende å lene seg på en «kjekt å ha»-mentalitet hvor irrelevante opplysninger behandles på lik linje som de relevante, med en tanke om at de på et senere tidspunkt kan fylle et, per nå, ukjent formål. I forhold til kriminalitetsbekjempelsen er dette særs viktig da prinsippet antyder at man ikke kan behandle opplysninger som er i strid med formålet, og at man på denne måten må være tydelig på hvilke opplysninger som er relevante for kriminalitetsbekjempelsen og hvilke som ikke er det.

---

[129] Schartum and Bygrave, *Personvern i informasjonssamfunnet*. Kapittel 2.4.4.2 side 67

[130] Schartum and Bygrave. Kapittel 2.4.4.2 side 68-69

3.2.3.2 Krav om behandlingskvalitet

For å ivareta opplysningskvaliteten må informasjonssystemene som behandler opplysningene og de rutinene som hører til informasjonssytemet ha en viss kvalitet. Dette betegnes som behandlingskvalitet. Slik kravet til behandlingskvalitet er beskrevet gjennom interesseteorien omtaler den en hel del typetilfeller som faller inn under behandlingskvalitet-begrepet. Blant annet skal informasjonssystemet som behandler personopplysninger kunne motstå forsøk på innbrudd (hacking) samtidig som systemet er stabilt i drift. Informasjonssystemet skal være enkelt å bruke, lett forståelig og til en viss grad kunne endres eller oppdateres uten at hele systemet må tas «offline». I tillegg til dette skal det ikke forekomme motstridende opplysninger i informasjonssystemene, opplysningene må kobles til riktig person og de opplysningene som ikke skal eller lar seg behandle må være utelatt eller utilgjengelig for informasjonssystemet i behandlingsprosessen[131]. På mange måter støtter kravet om behandlingskvalitet opp under kravet om opplysningskvalitet og til en viss grad i å ivareta det lovverket som er gjeldende. De fleste av disse typetilfellene gjør seg også gjeldende når man ser dem i sammenheng med kriminalitetsbekjempelsen. Kanskje særlig er risikoen knyttet til sikkerhetsbrudd i politiets informasjonssystemer å anse som det som kan skade kriminalitetsbekjempelsen mest. Man står da ovenfor et tilfelle hvor både politiets arbeid med kriminalitetsbekjempelse blir skadelidende og de som er registrert kan få sine opplysninger spredd eller misbrukt. Dette eksempelet reduserer ikke viktigheten av de andre typetilfellene og det er viktig å merke seg at kravet om behandlingskvalitet skal ivareta både den behandlingsansvarliges- og den registrertes plikter og retter.

3.2.4 Interessen i forholdsmessig kontroll

Den følgende interessen omhandler forholdsmessighet i kontrolltiltak. På flere områder i samfunnet utøves kontrolltiltak, både sporadisk og regelmessig. Schartum/Bygrave[132] skiller mellom kontroll og overvåkning. De beskriver kontroll som «de aktiviteter som gjelder innsamling av informasjon for å vurdere om folks handlinger er i samsvar med rettslige og sosiale handlingsnormer[133]». Dette gjelder eksempelvis kontroll av en persons skatteinnbetalinger for å unngå skattesnyltere. Overvåking beskriver de som «vedvarende eller systematisk innsamling av opplysninger, ved hjelp av personer, kameraer, bruk av aktivitetslogger, mv.[134]». Dette gjelder eksempelvis fartsskrivere i langtransport eller automatiske trafikkameraer som kontrollerer bilers fart, enten over en gitt avstand eller i øyeblikket. I be-

[131] Schartum and Bygrave. Side 70

[132] Schartum and Bygrave. Kapittel 2.4.5.1 side 73

[133] Schartum and Bygrave. Kapittel 2.4.5.1 side 73, andre avsnitt

[134] Schartum and Bygrave. Kapittel 2.4.5.1 side 73, tredje avsnitt

gge tilfellene av kontroll og overvåkning sees en forholdsmessighetsvurdering, hvor det hverken er ønskelig i et demokratisk samfunn med skattesnyltere eller langtransportsjåfører som kjører for lenge om gangen – kontrollen står i stil med den uønskede konsekvensen handlingen kan ha. Selv om det både er kontrolltiltak og overvåkning, sees det som nødvendig for å motvirke uønskede hendelser i samfunnet.

3.2.4.1 Kravet om forholdsmessighet mellom veiledning og kontroll

Det første kravet innenfor interessen i forholdsmessig kontroll er kravet om forholdsmessighet mellom veiledning og kontroll. I dette kravet ligger en forutsetning om at de fleste innbyggere ønsker å etterleve lovverket og unngå sanksjoner som følge av brudd på de handlingsnormer som foreligger. Det foreligger derfor en forholdsmessighet mellom det å sanksjonere noen eller føre kontroll med noen opp mot et krav til å veilede befolkningen slik at de lettere kan følge gjeldende handlingsnormer. Med særlig vekt på informasjonsarbeid og veiledning kan behovet for kontrolltiltak reduseres, da flere vil være kjent med det handlingsrommet som er akseptert. Hvorvidt dette er gjeldende for kriminalitetsbekjempelsen har jeg ingen empirisk grunnlag for å hevde, men en kan påpeke at det foreligger en stor mengde veiledning, gjerne gjennom media, som kan bidra til et redusert kriminalitetsbilde. Dess flere som er kjent med hva som er å anse som kriminelt, dess flere kan tenkes å ville innrette seg etter hva som er å anse som ikke-kriminelt.

3.2.4.2 Kravet om forholdsmessighet mellom forhåndskontroll og etterkontroll

Kravet om forholdsmessighet mellom forhåndskontroll og etterkontroll omtaler den behandlingsansvarliges plikt i å kvalitetssikre de opplysningene som behandles. En kontroll av opplysningenes kvalitet kan skje både før og etter at innsamlingen av opplysningene har funnet sted og det er den behandlingsansvarlige som må vurdere om det foreligger en god balanse mellom forhåndskontrollen og etterkontrollen. I utgangspunktet er forhåndskontroll av opplysninger å foretrekke, da kontrollen foregår i forkant av at selve behandlingen av opplysningene tar til. Dette skaper forutsigbarhet for den registrerte, såvel som at den behandlingsansvarlige kan være relativt sikker på at vedtaket som fattes på bakgrunn av opplysningene vil være korrekt. Når det kommer til kriminalitetsbekjempelsen brukes nok både før- og etterkontroll av opplysninger. Eksempelvis vil en polititjenestemann som gjennomfører en trafikkkontroll kunne sjekke om den aktuelle føreren har førerrett på bil i det føreren blir stoppet i kontrollen, isteden for å samle inn opplysninger om føreren for senere å avdekke hvorvidt føreren har førerrett eller ei. På den andre siden foregår mye av kriminalitetsbekjempelsen som reaktivt arbeid, altså arbeid etter at den kriminelle handlingen har blitt begått. Politiet og påtalemyndigheten blir da også bundet til å føre etterkontroll av de opplysningene som samles

inn i forbindelse med den kriminelle handlingen, med den hensikt å kvalitetssikre opplysningene og avdekke hvorvidt de er relevant. Dette blir særlig aktuelt i de tilfeller hvor gjerningspersonen er ukjent og politiet må samle inn opplysninger for å avdekke vedkommendes identitet, dette være seg gjennom analyser av biologisk materiale, trafikkdata på mobilnett mv.

3.2.4.3 Kravet om forholdsmessighet mellom kontroll til de registrertes gunst og til deres ugunst

Kravet om forholdsmessighet mellom kontroll til de registrertes gunst og til deres ugunst omtaler en mer prinsipiell eller ideologisk tanke om at kontrolltiltak ikke skal gjennomføres utelukkende for å påføre den registrerte sanksjoner, straff, bøter eller lignende. Dette er åpenbart ikke et forbud mot å iverksette kontrolltiltak som kan ha slike effekter – da ville det vært vanskelig å drive kriminalitetsbekjempende virksomhet. Det er likevel slik at den behandlingsansvarlige ikke skal, med bakgrunn i «egeninteresser», gjennomføre kontrolltiltak som påfører den registrerte ugunstige reaksjoner. Dette er kanskje særlig aktuelt i tilfeller hvor den behandlingsansvarlige har økonomisk gevinst av å gjennomføre kontrolltiltak mot den registrerte, eksempelvis i forsikringssaker. På den andre siden kan ulike kontrolltiltak ha positive effekter for den registrerte i form av at kontrollen kan utløse rettigheter for den registrerte som den registrerte ikke var klar over. Slike kontroller vil ha positive effekter for den registrerte, og kan ha «negative» effekter for den behandlingsansvarlige. Dette gjelder særlig innenfor områder av trygde- og sosialytelser. I alle tilfeller skal kontrolltiltakene være forholdsmessig vurdert. Når det kommer til kriminalitetsbekjempelsen vil dette i større grad være vanskelig å gjennomføre, altså å ikke skulle gjennomføre kontrolltiltak som kan ha negative konsekvenser for den registrerte. I mange tilfeller avdekkes kriminelle handlinger lenge etter at de er begått og oftest avdekkes disse ved hjelp av ny teknologi og politiets ulike kontrolltiltak. Med utgangspunkt i DNA-registeret kan politiet koble gamle, uløste saker opp mot en DNA-profil og således avdekke kriminelle handlinger lenge etter at de er begått. En slik kontroll er åpenbart ikke til den registrertes gunst, og det er også tvilsomt at samfunnet som sådan ønsker at slike kontroller ikke skal være mulig. Slik sett vil kravet om forholdsmessighet mellom kontroll til de registrertes gunst og til deres ugunst være vanskelig å forsvare opp mot kriminalitetsbekjempende virksomhet.

3.2.4.4 Kravet om forholdsmessighet mellom ekstern og intern kontroll

Kravet om forholdsmessighet mellom ekstern og intern kontroll omtaler forholdet mellom den behandlingsansvarlige og den registrerte. I noen tilfeller kan den registrerte ha interesse av å

oppgi feilaktige opplysninger ovenfor den behandlingsansvarlige, og den behandlingsansvarliges kontrolltiltak kan lett rettes utelukkende mot den registrerte. Kravet tilsier likevel at den behandlingsansvarlige også må gjennomføre kontrolltiltak internt i organisasjonen for å avdekke hvorvidt opplysningene er korrekte. For politiet og påtalemyndigheten foreligger det en vid adgang til å gjennomføre slike interne kontrolltiltak da de har tilgang til en stor mengde informasjon om personer gjennom ulike registre og nasjonale felleskomponenter. Således har den behandlingsansvarlige mulighet til å føre kontroll med opplysningene internt, før en eventuelt intensiverer kontrollen ovenfor den registrerte. Dette knytter seg godt opp mot kriminalitetsbekjempelsen da en som er mistenkt for en kriminell handling ikke alltid ønsker å oppgi korrekt informasjon ovenfor politiet og påtalemyndigheten, og det blir opp til den behandlingsansvarlige å føre interne kontroller av opplysningene for å avdekke deres invaliditet. På det tidspunkt at politiet og påtalemyndigheten er sikre på at opplysningene som den registrerte har gitt er feilaktige har de også grunnlag for å intensivere kontrolltiltakene ovenfor den registrerte.

3.2.5 Interessen i brukervennlig behandling

Interessen i brukervennlig behandling er til en viss grad noe selvforklarende – det er ønskelig at den registrerte blir møtt med respekt og tillit i alle tilfeller av behandlingen, både når behandlingen er frivillig og samtykkebasert og når den er lovpålagt og ikke ønsket av den registrerte. Interessen legger således opp til at samhandlingen mellom den behandlingsansvarlige og den registrerte skal være så god som mulig og at fravær av konflikt er ønskelig for et godt samarbeid. Med dette menes at både den behandlingsansvarlige og den registrerte kan og bør tilpasse seg på hver sin kant for å fremme en god tjeneste eller løsning. For å bedre forklare dette deles interessen i brukervennlig behandling opp i fire krav; krav om lydhørhet, krav om forståelighet, krav om uhindret dialog og krav om driftsstabilitet. I det følgende vil jeg gjøre rede for det enkelte krav og hvordan disse stiller seg med hensyn til kriminalitetsbekjempelsen.

3.2.5.1 Krav om lydhørhet

Kravet om lydhørhet omtaler at den behandlingsansvarlige skal ta hensyn til den registreres ønsker rundt hvordan opplysninger skal behandles og hvordan den behandlingsansvarlige skal ivareta den registrertes interesser. Slike individuelle tilpasninger forekommer på mange måter og som et eksempel kan nevnes muligheten for å unnta en persons fornavn i en offentlig søkerliste til en stilling for å ikke avsløre vedkommendes kjønn eller etnisitet. Dette er en individuell tilpasning som ikke nødvendigvis skader behandlingen av opplysninger og som på

den andre siden gir jobbsøkeren større sjanse for å ikke bli diskriminert på bakgrunn av kjønn eller etnisitet. Kravet om lydhørhet kan også gjelde en gruppe av registrerte og deres ønsker rundt hvordan den behandlingsansvarlige skal gjennomføre sitt virke. Oftest skjer dette gjennom den behandlingsansvarliges ønske om å skape bedre tjenester for sine brukere og tar ofte utgangspunkt i brukerundersøkelser eller lignende[135].

I forhold til kriminalitetsbekjempelsen er kravet om lydhørhet mindre aktuelt, da politiet og påtalemyndigheten i liten grad kan ta hensyn til hva den registrerte ønsker da dette kan påvirke kriminalitetsbekjempelsen i negativ retning. Individuelle tilpasninger til behandlingen av personopplysninger hos politiet vil sannsynligvis være i strid med flere rettssikkerhetprinsipper.

3.2.5.2 Krav om forståelighet

Kravet om forståelighet omhandler at informasjon som gis fra den behandlingsansvarlige til den registrerte skal være lett forståelig uavhengig av den registrertes kunnskapsnivå, og informasjonen bør også tilpasses i forhold til, eksempelvis, den registrertes alder. I praksis kan dette bety at et vedtak som er fattet av en behandlingsansvarlig kan måtte gis på et språk som den registrerte forstår eller inneholde et vedlegg som forklarer tydeligere hva vedtaket går ut på og innebærer.

Informasjon knyttet til kriminalitetsbekjempelsen bør også tilpasses den registrerte slik at vedkommende er kjent med sine rettigheter og plikter. Kravet om forståelighet knytter seg ofte opp mot innsynsretten og at dokumenter det gis innsyn i skal være forståelige. Det er likevel slik at innsynsretten i stor grad er unntatt med bakgrunn i kriminalitetsbekjempende virksomhet. I den grad det gis informasjon fra politiet til en registrert om kriminalitetsbekjempelsen, må denne da ifølge kravet være forståelig. Det er likevel noe vanskelig å se hvor dette har en praktisk verdi i min gjennomgang.

3.2.5.3 Krav om uhindret dialog

Krav om uhindret dialog omhandler hovedsaklig at det skal være enkelt for den registrerte å komme i kontakt med den behandlingsansvarlige, og da gjerne knyttet til oppfyllelsen av innsynsretten. I dette ligger det et krav om at den behandlingsansvarlige ikke kan kreve vederlag for å kunne kreve innsyn og at innsynsbegjæringer skal kunne leveres, eksempelvis, gjennom internett-baserte løsninger. Det skal videre være en forholdsmessighet mellom det å kunne få kontakt med den behandlingsansvarlige og den innsats som kreves for å oppnå denne kontakten. Hvis det er uforholdsmessig vanskelig å komme i kontakt med den behandlingsansvarlige

[135] Schartum and Bygrave. Kapittel 2.4.6.2 side 82, andre avsnitt

er ikke det ønskelig. Schartum/Bygrave[136] omtaler dette som «reduksjon av formelle og praktiske hindre som kan stå i veien for kontakten mellom de registrerte (..) og den behandlingsansvarlige (..).» Formelle hindre kan være en tvungen bruk av et skjema for å komme i kontakt med den behandlingsansvarlige, eller krav om betaling. Praktiske hindre er, som nevnt ovenfor, at den innsats som kreves for å komme i kontakt med den behandlingsansvarlige er så stor at det oftest ikke oppnås kontakt mellom den behandlingsansvarlige og den registrerte som en følge av dette. Dette betyr ikke nødvendigvis at alle hindre bør fjernes, da hindre kan ha sin hensikt. Dette gjelder eksempelvis i innsynsbegjæringer hvor det er viktig at det er klart hvem som begjærer innsyn, og at det da benyttes et bestemt skjema til dette formålet kan ikke sees som noe som hindrer kravet om uhindret dialog.

Med hensyn til kriminalitetsbekjempelsen er kravet om uhindret dialog delvis aktuelt. Generelt innsyn i politiregistre gis ved at den som ønsker innsyn fyller ut et skjema som sendes til politimyndigheten[137]. Utenfor straffesak kan den registrerte be om at Datatilsynet skal føre kontroll med Politiet og påtalemyndighetens behandling av opplysninger og sjekke om gjeldende lovverk etterleves. Dette er nærmere regulert i Politiregisterloven § 59[138] og etterkommer til dels kravet om uhindret dialog når det kommer til kriminalitetsbekjempelsen og ivaretakelse av den registrertes rettigheter.

3.2.5.4 Krav om driftsstabilitet

Kravet om driftsstabilitet omhandler at de systemene som behandler personopplysninger skal være stabile og driftssikre i den forstand at de skal ha en begrenset nedetid og at planlagte brudd i stabiliteten i minst mulig grad skal påvirke den registrertes interesser. Likeledes må systemene være i drift når behandlingen av opplysningene skal foregå.

Dette er særlig viktig når det kommer til kriminalitetsbekjempelsen, da politiet og påtalemyndigheten i stor grad benytter seg av datasystemer for å kunne føre kontroll med opplysninger i kriminalitetsbekjempende hensikt. I mange tilfeller foregår kriminalitetsbekjempelsen ute i ordenstjenesten, og det er kjent at politiet anvender digitale løsninger i ordenstjenesten. Dette omtales ofte som «politiarbeid på stedet[139]» og medfører bruk av ulike digitale hjelpemidler for å effektivisere politiarbeidet[140]. Dette inkluderer fjerntilgang til ulike politiregistre. For at slik type arbeid skal fungere må en forvente god driftsstabilitet i de løsningene som brukes.

---

136 Schartum and Bygrave. Kapittel 2.4.6.4, første avsnitt

137 Politiet, "Innsyn i politiets registre."

138 Justis- og beredskapsdepartementet, "Politiregisterloven." § 59

139 Politidirektoratet, "Politiarbeid på stedet."

140 Skarpenes, "Politiarbeid på stedet vil løfte politiet."

3.3 Empirisk relevans

Hvordan er så interesseteorien relevant for den empiri jeg baserer oppgaven min på? I de følgende delkapitlene vil jeg påpeke hvilke krav fra interesseteorien som gjør seg gjeldende i drøftingskapitlene for henholdsvis pool-ordningen, vandelskontroll og politiattest og internkontroll/informasjonssikkerhet. Kravene fra interesseteorien skal videre brukes for å analysere hvordan høringsinstansene har ment at forholdet mellom kriminalitetsbekjempelse og personvern bør vektes.

3.3.1 Pool-ordningen

Som beskrevet i kapittel 2.2 tillater pool-ordningen en fravikelse av kravene til formålsbestemthet, nødvendighet og relevans på inntil 4 måneder. I løpet av denne perioden, og så tidlig som mulig, skal opplysningene som behandles etter denne bestemmelsen avklares med henhold til kravene om formålsbestemthet, nødvendighet og relevans. Hvis dette ikke oppnås innenfor perioden på 4 måneder må opplysningene behandles på et annet rettslig grunnlag eller slettes fra registrene.

Når det kommer til interesseteorien er det særlig kravene om opplysnings- og behandlingskvalitet som gjør seg gjeldende når jeg skal analysere høringssvarene fra høringsrunden til NOU 2003:21 angående pool-ordningen.

3.3.2 Vandelskontroll og politiattest

Bestemmelser knyttet til bruk og utstedelse av vandelskontroller og politiattester er regulert i Politiregisterlovens kapittel 7. Det som kjennetegner vandelskontroll og politiattester er at de i mange tilfeller inneholder sensitive personopplysninger og at de har et relativt utstrakt bruksområde. Det foreligger også utfordringer knyttet til personvernet når det kommer til vandelskontroller og politiattester.

Interesseteoriens krav om opplysnings- og behandlingskvalitet, kravet om vern av individets identitetsbilde, og kravet om uhindret dialog er relevante i den videre analysen.

3.3.3 Informasjonssikkerhet/sporbarhet

Internkontroll er et verktøy som skal hjelpe den behandlingsansvarlige med å være i overenstemmelse med de lover og regler som gjelder for den behandling av personopplysninger som foregår i den aktuelle virksomhet. Med dette menes opprettelse og etterlevelse av interne rutiner for hvordan personopplysninger eksempelvis skal behandles i forbindelse med en innsynsbegjæring eller ved utstedelse av en politiattest. Internkontrollen er ment å ivareta både den registrertes- og den behandlingsansvarliges rettigheter og plikter. Informasjonssikkerhet er et internkontrollteknisk tiltak som skal besørge konfidensialitet, integritet og tilgjengelighet i

informasjonssystemer. Som et informasjonssikkerhetstiltak skal jeg ta for meg sporbarhet i elektroniske systemer, som i hovedsak handler om logging av brukeraktivitet.

Interesseteoriens krav til forholdsmessig kontroll fremstår som den mest relevante interessen når det kommer til analysen av høringsinstansenes syn på internkontroll og informasjonssikkerhet. I tillegg kommer kravet om behandlingskvalitet, kravet om konfidensialitet og kravet om et etablert tillitsforhold.

4 Drøftinger

Med utgangspunkt i høringsuttalelsene knyttet til NOU 2003:21[141] viser det seg en del gjennomgående tematikk som flere av høringsinstansene merker seg ved. Pool-ordningen, politiattester og informasjonssikkerhet/sporbarhet utmerker seg som tre kjernepunkter fra høringsuttalelsene.

I de følgende kapitlene vil jeg gjøre rede for hva høringsinstansene mente om henholdsvis pool-ordningen, politiattester og informasjonssikkerhet/sporbarhet. Videre skal jeg anvende teorien jeg har gjort rede for ovenfor for å analysere hvordan høringsinstansene mente at forholdet mellom kriminalitetsbekjempelse og personvern skulle ivaretas i lovforslaget. På denne måten kan jeg se hvilke aktørgrupper som fremmet hvilke meninger og om høringsinstansene hadde meninger om vektingen av forholdet mellom kriminalitetsbekjempelse og personvern. Samtidig vil jeg se om høringsinstansenes argumenter kan knyttes opp mot interesseteoriens ulike krav.

Drøftingene i kapitlene 5 til 7 vil således deles i to. Kapitlene 5.1, 6.1 og 7.1 vil vekselsvis inneholde beskrivelser og gjengivelser av høringsinstansenes syn på de ulike kjernepunktene.

Kapitlene 5.2, 6.2 og 7.2 er kapitler hvor jeg anvender interesseteorien fra kapittel 3.2 for å analysere høringsinstansenes merknader til kjernepunktene. Interesseteorien vil jeg anvende på kravsnivå – altså et mer detaljert nivå innenfor hver av interessekategoriene. Dette innebærer at ikke alle deler av interesseteorien, eller alle krav innenfor interesseteorien, tas med i vurderingene. Dette er enten grunnet i at kravet fra interesseteorien ikke kan gjenfinnes i høringsinstansenes uttalelser, eller at interesseteorien ikke lar seg anvende på høringsinstansenes uttalelser.

I kapitlene 5.3, 6.3 og 7.3 gjør jeg rede for om de tre kjernepunktene, høringsuttalelsene og kravene fra interesseteorien later til å vektlegge kriminalitetsbekjempelse mer enn personvern, og vice versa. Dette baseres på mine vurderinger og observasjoner gjennom arbeidet med høringsuttalelsene og interesseteorien.

De høringsinstansene som omtales i de følgende kapitlene er de som ytret noe relevant i forbindelse med de ulike kjernepunktene. Høringsuttalelser som er utelatt, er utelatt da de ikke inneholder relevante bemerkninger for pool-ordningen, politiattester eller informasjonssikkerhet/sporbarhet.

[141] Justis- og politidepartementet, JD, "NOU 2003:21."

5 Pool-ordningen

Pool-ordningen[142], eller 4-måneders regelen, tillater politiet og påtalemyndigheten å behandle personopplysninger uten rettslig grunnlag i inntil fire måneder før de må avgjøre om opplysningene er korrekte eller relevante for det formålet de er innsamlet. Denne ordningen er særlig tiltenkt å dekke et behov for å kvalitetssikre opplysninger som tilkommer politiet, men som ikke lar seg verifisere uten ytterligere etterforskning. Dette omfatter alt fra opplysninger som tilkommer politiet via tips fra publikum, til opplysninger som politiet selv avdekker som følge av en etterforskning eller i forbindelse med et lovbrudd. Lovverket omtaler det som kravene til formål, nødvendighet og relevans. Tidsbegrensningen gjelder likevel ikke når det kommer til behandling av opplysninger i den enkelte straffesak. Med dette menes at opplysninger som fremkommer som en del av en straffesak kan behandles så lenge straffesaken verserer uten at kravene til formål[143],nødvendighet[144] eller relevans[145] er oppfylt.

5.1 Høringsinstansenes syn på Pool-ordningen

Med hensyn til Pool-ordningen har flere av høringsinstansene ulike syn på utfordringer knyttet til denne ordningen. Flere av politidistriktene, samt Kripos og Politidirektoratet, anser at fire måneder som tidsfrist for pool-ordningen er for kort. De argumenterer at det i flere tilfeller kan ta lengre tid å avklare en opplysnings relevans, formål og nødvendighet og at de således blir tvunget til å slette opplysninger før de har blitt anvendt eller vurdert. Dette kan også forringe kriminalitetsbekjempelsen i deres øyne og det fremstilles som et ressursproblem.
KRIPOS påpeker i sin uttalelse[146] at fristen på fire måneder, som Pool-ordningen legger opp til, er for kort. De begrunner dette på flere måter, blant annet i at noen politidistrikt har for

[142] Se kapittel 2.3.1 for en utdypende redegjørelse av pool-ordningen

[143] Formålsbestemthetsprinsippet omhandler at opplysninger skal behandles til det formålet de er innsamlet. Hvis opplysninger skal behandles med et nytt formål som ikke er forenlig med det formålet opplysningene opprinnelig var innsamlet til, skal det bes om samtykke til at opplysningene behandles til et nytt formål, eventuelt må opplysningene samles inn på nytt til det nye formålet.

[144] Nødvendighetsprinsippet omhandler at det ikke skal innsamles eller behandles mer opplysninger enn det som er nødvendig for å kunne oppfylle formålet med behandlingen. Opplysningene må også være nødvendig å behandle for å oppfylle formålet med behandlingen. Det skal altså ikke behandles opplysninger som ikke er nødvendig for å oppnå formålet med behandlingen.

[145] Med relevans menes at opplysningene som behandles må ha en logisk sammenheng med formålet med behandlingen. Eksempelvis er det en logisk sammenheng mellom å behandle skatteopplysninger og avdekking av skattefusk, mens det derimot ikke er logisk sammenheng mellom å behandle opplysninger om en persons etnisitet og skattefusk.

[146] Kriminalpolitisentralen (KRIPOS), Frigaard, and Wiese Bromander, Høringsuttalelse - NOU 2003:21 - Kriminalitetsbekjempelse og personvern - politiets og påtalemyndighetes behandling av opplysninger.

knappe ressurser til å møte kravet etter loven og at fristen ikke legger opp til muligheter for å «sjekke noen ut» av en sak. Den antagelige årsaken til at KRIPOS anser tidsfristen som et ressursproblem er at politiet behandler store mengder opplysninger, og i mange tilfeller gjøres dette av polititjenestemenn. Når mengden av opplysninger som befinner seg i pool-ordningen skal klareres med tanke på formål, nødvendighet og relevans krever dette tilsvarende store mengder personellressurser. Slik KRIPOS legger frem sine synspunkter later det til at disse personellressursene ikke er tilgjengelige, og slik tidsfristen foreligger vil politiet måtte slette opplysninger som kan være verdifulle før de har kunnet avgjøre verdien av dem. Videre henviser de også til den enkeltes rettssikkerhet, da det ikke skal være slik at uskyldige skal måtte være i politiets søkelys over lengre tid. Til slutt bemerker KRIPOS at Pool-ordningen er hentet fra Nederland som, ifølge KRIPOS, erfaringsmessig er vanskelig å samarbeide med da nederlandske politimyndigheter ofte har slettet informasjon som norsk politi etterspør.

Oslo Politidistrikt påpeker i all hovedsak mye av det samme som KRIPOS i sin høringsuttalelse[147]. De omtaler effektivitetshensyn, hensyn til sikkerhet i den operative tjenesten og risikoen for at verdifull informasjon slettes før den kan avklares. Oslo Politidistrikt påpeker at slik lovforslaget foreligger er bestemmelsene egnet til å tilfredsstille politiets behov for å kvalitetssikre informasjon. De bemerker også at reglene i loven må være fornuftige og praktikable i den grad at de ikke er til hinder for en effektiv bekjempelse av kriminalitet. Med «fornuftig og praktikable» antar jeg at politiet mener at reglene i loven på best mulig måte bør understøtte deres arbeid med kriminalitetsbekjempende virksomhet og at reglene således enkelt kan utføres i praksis av de polititjenestemenn som samler inn opplysninger. Hva som er «fornuftige regler» i politiets øyne er ikke nødvendigvis fornuftige i andres øyne. Det ligger likevel en antydning i distriktets uttalelse om at reglene ikke bør være til hinder for deres kjernevirksomhet og at reglene på denne måten er «fornuftige».

Troms Politidistrikt påpeker i sin høringsuttalelse at *«en manuell oppfølging av (pool-ordningen) vil både bli arbeidskrevende og lite nøyaktig.[148]»*
I dette mener Troms Politidistrikt at personellressurser kan bli låst fast i behandling av opplysninger som samles inn som en del av pool-ordningen. De later således til å ønske seg at

147 Oslo Politidistrikt and Halvorsen, Høring - NOU 2003:21 - Politiregisterutvalget.

148 Troms Politidistrikt, Isaksen, and Bredrup Sæverud, Høring - NOU 2003:21 Kriminalitetsbekjempelse og personvern.

opplysningene kan behandles automatisk av et datasystem, både for å frigjøre personellressurser og for å sikre enhetlig og nøyaktig behandling av opplysningene.

ØKOKRIM (Den sentrale enhet for etterforskning og påtale av økonomisk kriminalitet og miljøkriminalitet) påpeker i sin høringsuttalelse[149] at et av deres hovedansvarsområder, hvitvasking, i liten grad kan reguleres gjennom politiregisterloven. De begrunner dette i det store antallet meldinger de får som må undersøkes i forhold til hvitvasking, og at de vil ha vansker med å gjennomføre tilstrekkelig informasjonsinnhenting i løpet av de fire månedene, som loven legger opp til, for å kunne avdekke eventuelle straffbare handlinger.

Politiets Sikkerhetstjeneste (PST) på sin side bemerker tilfredshet med pool-ordningen slik den foreslås. De mener at pool-ordningen vil tilfredsstille deres behov i innsamlingsfasen. I tillegg påpeker de verdien av pool-ordningen som et verktøy for å styrke virksomhetens forhold til internkontroll. I dette ligger det at kravene som stilles med hensyn til pool-ordningen tvinger den behandlingsansvarlige til å ha kontroll med de opplysningene som er registrert. Dette gjelder særlig forholdet til tidsfristen på 4 måneder, da opplysninger som ikke er avklart innen tidsfristen skal slettes. Ved hjelp av gode internkontrollrutiner kan PST bedre ha oversikt over hvilke opplysninger det er mest prekært å avklare og hvilke som må slettes innen tidsfristen.
I PSTs høringsuttalelse[150] uttrykkes det ikke eksplisitt hva som er grunnlaget for at de er tilfreds med pool-ordningen slik den foreslås, foruten at bestemmelsen gir PST tilstrekkelig tid til å vurdere de ikke-verifiserte opplysningene og hvorvidt de oppfyller kravene til formålsbestemthet, nødvendighet og relevans.
Felles for høringsuttalelsene fra KRIPOS, politidistriktene, ØKOKRIM og PST er at det er politifaglige begrunnelser som ligger til grunn for argumentene de presenterer. I svært liten grad blir forholdet til personvern nevnt, og blant annet KRIPOS sier at en utvidelse av 4-månedersregelen vil ha liten betydning for personvernet opp mot den gevinst denne ordningen kan ha.
Politiets Data-og Materiellteneste (PDMT[151]) bemerker i sin høringsuttalelse[152] fra den systemtekniske siden at de teknologiske løsningene som er i bruk er av eldre dato og at de i

[149] ØKOKRIM and Einar Høgetveit, Høring - NOU 2003: 21 Kriminalitetsbekjempelse og personvern.

[150] Politiets Sikkerhetstjeneste (PST), Øverkil, and Welhaven, Høringsuttalelse - NOU 2003:21 Kriminalitetsbekjempelse og personvern.

[151] Idag er PDMT delt i to; Politiets Fellestjenester og Politiets IKT-tjenester

[152] Politiets Data- og Materiellteneste (PDMT) and Bøhler, Kriminalitetsbekjempelse og personvern - Høring.

varierende grad inneholder blant annet automatiserte saneringsrutiner. Likt som Troms Politidistrikt er dette en bemerkning om at et manuell oppfølging av pool-ordningen vanskelig lar seg gjennomføre, og at det således er ønskelig med automatiserte saneringsrutiner. PDMT påpeker likevel at systemene som behandler opplysninger i varierende grad inneholder automatiserte saneringsrutiner, og at datasystemene i liten grad kan enkelt oppgraderes for å oppfylle lovens krav om saneringsrutiner. For å oppfylle lovens krav knyttet til pool-ordningen kreves det, ifølge PDMT, store oppgraderinger på systemsiden.

Fra den ikke-politifaglige siden er det svært få høringsuttalelser som tar for seg pool-ordningen.

Datatilsynet[153] anviser at den registrertes/befolkningens personvern må være viktigere enn pool-ordningen. De bemerker at politiet og påtalemyndigheten i det minste bør ha en viss formening om en opplysnings relevans når opplysningen samles inn – altså om det foreligger en logisk sammenheng mellom opplysningene og formålet de er innsamlet til. De påpeker videre at fire måneder er en for vid tidsramme, da det også er åpning for å utlevere opplysninger fra pool-ordningen – opplysninger som ikke er verifiserte. Dette mener Datatilsynet truer personvernet, særlig med tanke på opplysningskvalitet og den skade uriktige opplysninger kan påføre den registrerte. En forstår det slik at Datatilsynet opplever pool-ordningens bestemmelser med fordel kunne vært innskrenket for å bedre kunne ivareta personvernet, samtidig som Datatilsynet anerkjenner at Politiet i tilfeller må kunne behandle ikke-verifiserte opplysninger som et del av sitt arbeide.

Advokatforeningen[154] omtaler forslaget til ny politiregisterlov i særlig positive ordelag. De opplever at balansen mellom kriminalitetsbekjempelse og personvern er godt ivaretatt gjennom lovforslaget. I tillegg ser de at regelverket er moderne nok til å tilpasses fremtidig teknologi, samtidig som den tilfredsstiller internasjonalt lovverk. De påpeker også at innføringen av personvernrettslige prinsipper, som nødvendighet og formålsbestemthet, er særlig positivt for å best kunne ivareta den enkeltes personvern. Advokatforeningen mener også at pool-ordningen er nødvendig for politiets virksomhet.

---

153 Datatilsynet, Apenes, and Gulbrandsen, HØRINGSUTTALELSE.NOU 2003:21 KRLMINALITETSBEKJEMPELSE OG PERSONVERN.

154 Den Norske Advokatforening, Aarseth, and Smith, Høringssuttalelse - NOU 2003:21 Kriminalitetsbekjempelse og personvern.

5.2 Pool-ordningen vs. Krav fra interesseteorien

I det følgende vil jeg anvende teori på den informasjonen jeg har hentet ut fra høringsuttalelsene og vurdere disse opp mot teorien. Jeg har plukket ut enkelte krav fra interesseteorien som jeg mener er relevante å se på opp mot pool-ordningen og bruker således ikke hele interesseteorien for å gjøre mine analyser. For pool-ordningen sin del har jeg plukket ut to krav fra interesseteorien og disse vil utgjøre underkapitlene videre.

5.2.1 Krav til opplysningskvalitet

Som tidligere nevnt omhandler pool-ordningen en mulighet for politiet og påtalemyndigheten å se bort ifra kravene til opplysningers formål, relevans og nødvendighet i en periode på inntil fire måneder. Opplysningene som innsamles med hjemmel i denne bestemmelsen skal så snart som mulig undergå kvalitetskontroll for å avdekke opplysningenes formål, relevans og nødvendighet, før de eventuelt brukes videre med et annet hjemmelsgrunnlag. Hvis det ikke foreligger hjemmelsgrunnlag i løpet av denne perioden på fire måneder skal opplysningene slettes. Dette er opplysninger som i utgangspunktet skal bidra i politiets og påtalemyndighetens arbeid med kriminalitetsbekjempelse og er således ikke å anse som å være en del av en aktuell straffesak.

Politietaten selv omtaler i liten til ingen grad utfordringer knyttet til opplysningskvalitet i sine høringsuttalelser.

Datatilsynet på sin side påpeker at politiet og påtalemyndigheten i det minste bør ha en formening om opplysningenes relevans når det kommer til pool-ordningen. Med dette mener Datatilsynet at det bør foreligge en logisk sammenheng mellom det opplysningen gir av informasjon og det formålet som opplysningene skal brukes til. Spørsmålet er således om opplysningen er egnet til å fylle formålet med behandlingen.

Ved første øyekast later ikke pool-ordningen til å oppfylle interesseteoriens krav om opplysningskvalitet. De opplysningene som behandles i pool-ordningen kan ha en begrenset eller uavklart grad av validitet - altså grad av presisjonsnivå, grad av fullstendighet og grad av riktighet. I dette ligger det at opplysningene i pool-ordningen ikke alltid gir en god representasjon av det de er ment å beskrive, være seg en person, en hendelse eller et kjøretøy mv. Særlig kan dette gjelde opplysninger som tilkommer politiet gjennom tips fra befolkningen, da det eksempelvis ikke alltid er lett å se forskjell på en sort eller en mørkeblå jakke i de sene nattetimer. Dette påvirker naturligvis opplysningenes validitet, eller grad av korrekthet. I anledning pool-ordningen har lovgiver dermed valgt en litt annen tilnærming til kravet til opplysningskvalitet. Dette gjenspeiler seg i Politiregisterlovens § 6[155] siste ledd hvor kravet til opplys-

[155] Justis- og beredskapsdepartementet, "Politiregisterloven." § 6 siste ledd

ningskvalitet er at opplysningene «gjengis slik kilden ga dem». Således kan en hevde at opplysningene har en subjektiv god kvalitet fra kildens side, mens det er politiets oppgave å gjøre rede for den objektive kvaliteten på de samme opplysningene gjennom etterforskning og ytterligere politiarbeid.

Nå er kanskje ikke tilfellet med forskjellen på blå eller sort jakke det beste eksempelet på en opplysning som blir behandlet i pool-ordningen, men eksempelet illustrerer likevel på hvilken måte kravet om opplysningskvalitet er forsøkt oppnådd i lovgivningen. Tilfellet vil i stor grad være det samme om opplysningene det gjelder er av en mer personvernsensitiv art, være seg kjønn, hudfarge, geografisk plassering, biometriske data mv.

5.2.2 Krav til behandlingskvalitet

I tett sammenheng med kravet til opplysningskvalitet finner vi kravet til behandlingskvalitet. For pool-ordningen sin del er det flere høringsinstanser som påpeker utfordringer knyttet til behandlingskvalitet. Politiets Data- og Materielltjeneste påpeker at mange av systemene som behandler opplysninger er av eldre dato og at få av dem har innebygde saneringsrutiner. Dette er særlig viktig da opplysninger som behandles med hjemmel i pool-ordningen skal slettes hvis de viser seg å ikke møte kravene til formålsbestemthet, nødvendighet og relevans. Ett av politidistriktene påpeker at en manuell oppfølging av saneringsrutiner knyttet til pool-ordningen er særdeles arbeidskrevende og i værste fall vanskelig gjennomførbart.

Det uttrykkes således bekymring fra politietatens side når det kommer til ivaretakelsen av kravet til behandlingskvalitet, og da spesielt i tilknytning til sletterutiner med hensyn til pool-ordningen.

Fra et personvernperspektiv er det et viktig prinsipp at opplysninger om en selv som ikke er korrekte, oppdaterte eller relevante skal kunne kreves rettet eller slettet. Hovedtanken er at det ikke skal være slik at beslutninger eller vedtak blir fattet på et uriktig grunnlag, og det er særlig relevant når det kommer til personopplysninger som grunnlag for slike beslutninger eller vedtak. Likeledes skal ikke noen måtte lide under trykket av en mistanke fra politiets side i lang tid, særlig hvis dette viser seg å være urettmessig. I det opplysningene som var grunnlaget for mistanken viser seg å være feilaktige eller irrelevante skal opplysningene fjernes, sammen med mistanken. Slik er det også for pool-ordningen.

Som en del av kravet til behandlingskvalitet omtales også betegnelsen «registreringskvalitet[156]».

[156] Schartum and Bygrave, *Personvern i informasjonssamfunnet*. Side 70

Registreringskvalitet har fire aspekter;

- i hvilken grad nødvendige personopplysninger er registrert i informasjonssystemet;
- i hvilken grad personopplysninger det ikke er adgang til å behandle, er utelatt fra informasjonssystemet;
- i hvilken grad det er fravær av flere og ikke konsistente personopplysninger av samme type i systemet;
- i hvilken grad det benyttes korrekte og tilstrekkelige identifikasjonskoder for hver registrert personopplysning

De tre første aspektene sier noe om opplysningenes konsistens – altså hvorvidt opplysningene som skal beskrive en og samme person faktisk gjør dette uten å motsi hverandre. Det siste aspektet sier noe om opplysningenes identifiserbarhet – altså hvordan opplysningene skal tolkes og forstås slik at riktig opplysning knyttes til riktig person. I pool-ordningen er nettopp registreringskvalitet noe vanskelig da store deler av de overnevnte aspektene fravikes som en del av ordningen. Etter hva jeg kan forstå kan *alle* typer opplysninger behandles i pool-ordningen, opplysningene er uavklart og det er ikke nødvendigvis kjent til hvem eller hvor de enkelte opplysningene tilhører.

5.3 Vektlegges kriminalitetsbekjempelsen eller personvernet?

Med utgangspunkt i de overstående analysene av høringsinstansenes uttalelser er det relativt tydelig for meg at det er kriminalitetsbekjempelsen som vektlegges hos høringsinstansene når det kommer til pool-ordningen. Pool-ordningen i seg selv er ikke et verktøy som skal besørge godt personvern, men heller et verktøy som skal brukes i tilknytning til politiets- og påtalemyndighetens kjernevirksomhet.

Pool-ordningen fraviker tradisjonelle personvernprinsipper som formålsbestemtshetsprinsippet, nødvendighetsprinsippet og kravet til relevans. Ordningen kan således sees som et carte blanche for politiet og påtalemyndigheten i inntil 4 måneder før de tradisjonelle personvernprinsipper gjør seg gjeldende igjen. Samtidig er kravet om opplysningskvalitet modifisert[157] for å bedre passe inn i ordningen.

Høringsinstansene fra politiet og påtalemyndigheten stiller seg stort sett positive til pool-ordningen og ønsker seg i flere tilfeller «mer av det gode» - eksempelvis utvidet lagringstid før opplysningene må vurderes mv. Politietaten selv tar i liten grad opp personvernmessige aspekter eller utfordringer knyttet til pool-ordningen, og det blir ved flere anledninger benyttet politifaglige argumenter for viktigheten av denne ordningen.

Fra den ikke-politifaglige siden finnes det noen få som bemerker viktigheten av å ivareta personvernet i en slik løsning. Blant annet Datatilsynet viser i sin uttalelse at det er både den

[157] «Opplysningene gjengis slik kilden ga dem»

registrertes personvern og polititjenestemennenes personvern som må ivaretas i en slik ordning.

Med tanke på at pool-ordningen fremstår som et verktøy for å bistå i kriminalitetsbekjempelsen, må fokuset på personvern ivaretas på andre måter – så langt det er mulig. Særlig bør det være et fokus på god behandlingskvalitet, slik interesseteorien beskriver det. Med dette menes eksempelvis at det finnes rutiner for hvordan opplysninger skal føres med hjemmel i pool-ordningen, at det er tydelig hvem som har ført opplysningene inn i systemet, at det er et begrenset antall personell som kan føre opplysninger inn i registrene, at de som har skriverett i registrene er godt opplært og kurset og at opplysningenes integritet ivaretas på best mulig måte gjennom internkontroll- og informasjonssikkerhetstiltak.

Slike betraktninger er likevel i liten til ingen grad tematisert av høringsinstansene med tanke på pool-ordningen.

6 Vandelskontroll og politiattest

Vandelskontroll og politiattest har til hensikt å gjøre rede for hvorvidt en person er egnet til å inneha en stilling, verv eller arbeide. De brukes også i strafferettspleien for å kunne gjøre rede for en tiltalts straffehistorikk.

Som nevnt i kapittel 2.3.3 innebærer bruken av vandelskontroll og utstedelser av politiattester at personopplysninger må behandles. Oftest er disse opplysningene å anse som sensitive personopplysninger. Det er også slik at stadig flere arbeidsgivere mv. ønsker å bruke politiattester for å være sikre på at «den riktige» blir ansatt eller får stillingen.

I det følgende vil jeg gjøre rede for høringsinstansenes syn på vandelskontroll og politiattester. Videre vil jeg anvende teori på høringsinstansenes syn, for til slutt å gjøre en vurdering av hvorvidt det er kriminalitetsbekjempelsen eller personvernet som vektlegges i høringsinstansenes merknader.

6.1 Høringsinstansenes syn på vandelskontroll og politiattest

Siden reguleringen av vandelskontroll og politiattest er samlet i ett lovverk, politiregisterloven, er det mange av høringsinstansene som omtaler dette temaet. De fleste fremmer sine ansvarsområder som viktige, særlig i forbindelse med utstedelse av politiattest for personer som skal arbeide med barn, være seg i barnehage/skole, barnevern eller fritidsaktiviteter.
Kommunal- og regionaldepartementet[158], Barneombudet[159] og Utdannings- og forskningsdepartementet[160] påpeker i sine høringsuttalelser viktigheten av å kunne ivareta barn og unge i skole, fritidsaktiviteter og i asylmottak. De bemerker at barn er særdeles sårbare i slike situasjoner, og at det således er viktig at lovverket tar høyde for å skape en beskyttelse for barn i disse delene av samfunnet. I anledning bruk av vandelskontroll og politiattest påpeker høringsinstansene at lovverket bør inneholde en mulighet for å kunne avkreve politiattest for personer som skal arbeide med, eller omgås, barn og unge

Politietaten har gjennom sine høringsuttalelser flere bemerkninger å komme med når det gjelder vandelskontroll og politiattester.

---

158 Kommunal- og regionaldepartementet, Finstad, and Grønvold, NOU 2003:21 - Kriminalitetsbekjempelse og personvern - Høring.

159 Barneombudet, Haanes, and Storm Thorstensen, Høringssvar: NOU 2003:21 Kriminalitetsbekjempelse og personvern.

160 Utdannings- og forskningsdepartementet, Lauvås, and Israelsson, NOU 2003: 21 Kriminalitetsbekjempelse og personvern - horing.

Oslo Politidistrikt[161] sier seg tilfreds med måten lovforslaget gir generelle bestemmelser om hvilke formål som gir rett til bruk av politiattester. De begrunner dette i at det er andre enn politiet som er mottakere av informasjonen som gjengis i en politiattest - at det således er et spørsmål om hva politiets ressurser skal brukes til. Dette gjelder særlig da flere og flere yrkesgrupper legger opp til bruk av politiattest og nettopp dette skaper merarbeid for politiet. Da lovforslaget legger opp til generelle bestemmelser knyttet til hvilke formål en politiattest er berettiget, ser Oslo Politidistrikt bestemmelsene knyttet til vandelskontroll og politiattest som et hensiktsmessig verktøy.

Romerike Politidistrikt påpeker i sin uttalelse[162] at lovforslaget kan bidra til bedre forutsigbarhet for den enkelte når det kommer til bruk av vandelskontroll og politiattester, og den enkelte kan i større grad selv gjøre seg kjent med de lover og regler som gjelder. Samtidig påpeker de et behov for økte ressurser for å oppfylle lovens krav rundt fornyelse av politiattester.
Rogaland Politidistrikt bemerker i sin høringsuttalelse[163] at de foreslåtte bestemmelsene om vandelskontroll og politiattest fordrer økt ressursbruk på politiets side, og at slike ressurser må enten tildeles eller omdisponeres innenfor det enkelte politidistrikt.

Hordaland Politidistrikt uttaler[164], i likhet med Romerike Politidistrikt, tilfredshet med at bestemmelsene knyttet til vandelskontroll og politiattest nå gjøres mer tilgjengelige og oversiktlige. De er videre av den oppfatning at bestemmelsene vil medføre økt ressursbruk og -behov, og de foreslår at det bør kunne innføres et utstedelsesgebyr knyttet til politiattester, kanskje særlig når disse kan fornyes hvert 3.år.
Gudbrandsdal Politidistrikt bemerker i sin uttalelse[165] at regelendringer som lovforslaget legger opp til oftest medfører merarbeid utover det som er antatt på forhånd. Slikt merarbeid kan også gå utover politiets kjerneoppgaver, ifølge politidistriktet.

[161] Oslo Politidistrikt and Halvorsen, Høring - NOU 2003:21 - Politiregisterutvalget.

[162] Romerike politidistrikt and Plathe Maartmann, Høring - NOU 2003:21 - Kriminalitetsbekjempelse og personvern - politiets og påtalemyndighetes behandling av opplysninger.

[163] Rogaland politidistrikt, Sønderland, and Andersen, NOU 2003:21 - Kriminalitetsbekjempelse og personvern - politiets og påtalemyndighetes behandling av opplysninger - Høring.

[164] Hordaland Politidistrikt, Refvik, and Krogvold, Høring - NOU 2003:21 Kriminalitetsbekjempelse og personvern - Politiets og påtalemyndighetens behandling av opplysninger.

[165] Gudbrandsdal Politidistrikt and Sørby, Høring - NOU 2003:21 Kriminalitetsbekjempelse og personvern.

Østfold Politidistrikt uttaler[166] at straffesaker som er avgjort i konfliktrådsbehandling bør kunne påføres en uttømmende politiattest. De viser til at samfunnsmessige hensyn bør tale for en slik løsning, da interessene som ligger bak ordningen med uttømmende politiattest sees som viktigere enn å ikke påføre eventuelle avgjørelser fra en konfliktrådsbehandling.

KRIPOS bemerker en spesifikk problemstilling knyttet til vandelskontroll og kriminalitetsbekjempelse;
«Vandelskontroll gjelder den person som er aktuell i forhold til den stilling, funksjon m.v. som ønskes besatt. Ut fra de erfaringer som er gjort, er man ikke bekvem med denne situasjonen. Man har hatt situasjoner hvor enkelte kriminelle grupper eller enkeltpersoner søker å få innpass i organisasjoner eller på arbeidsplasser, ved å få tilsatt en person som står i nær relasjon til vedkommende, eksempelvis samboer av et medlem av en kriminell motorsykkelklubb. Både med dagens lovverk og det foreslåtte lovverk, er dette situasjoner som vanskelig lar seg fange opp, og hvor spørsmålet om hjemmel til å vurdere dette ikke er drøftet. Som et resultat av dette vil det etterhvert kunne oppstå lokale «ad-hoc»-løsninger, for å imøtekomme dette problemet. Det kan ikke være ønskelig, og lovgiver bør dermed gå foran for å løse dette.[167]»
Felles for høringsuttalelsene fra politietaten er forholdet til økt ressursbehov og økt arbeidsmengde. I tillegg antydes det til «smutthull» i lovverket som etaten ønsker å motvirke. Likevel berømmes Politiregisterutvalgets fokus på å samle bestemmelser knyttet til vandelskontroll og politiattester og at dette vil skape bedre forutsigbarhet for den enkelte, samtidig som bestemmelsene kan forhindre en økende grad av vilkårlighet når det kommer til vandelskontroller og politiattester.

Tilsynsmyndighetene har på sin side flere bemerkninger av ulik karakter. Datatilsynet[168] på sin side bemerker at resultatene av en vandelskontroll eller lignende oftest har stor betydning for den kontrollen gjelder. De påpeker således viktigheten av et klart hjemmelsgrunnlag for når vandelskontroll kan benyttes, mv. Datatilsynet stiller også spørsmål ved hvorvidt kvaliteten på dataene som brukes i en uttømmende politiattest ikke vil forringes over tid. De mener således at opplysningene som fremkommer i en uttømmende politiattest vil kunne endre

[166] Østfold politidistrikt, Lien, and Arnesen, Høring - NOU 2003:21 - Kriminalitetsbekjempelse og personvern.

[167] Kriminalpolitisentralen (KRIPOS), Frigaard, and Wiese Bromander, Høringsuttalelse - NOU 2003:21 - Kriminalitetsbekjempelse og personvern - politiets og påtalemyndighetes behandling av opplysninger.

[168] Datatilsynet, Apenes, and Gulbrandsen, HØRINGSUTTALELSE.NOU 2003:21 KRLMINALITETSBEKJEMPELSE OG PERSONVERN.

kvalitet over tid, og dermed risikere å gi et uriktig eller ufullstendig bilde av det attesten er ment å gjøre rede for. De bemerker videre at tilfredsstillende datakvalitet er et grunnleggende prinsipp innenfor personvernretten.

Helsetilsynet påpeker i sin høringsuttalelse[169] at tilsynsmyndigheten selv bør kunne innhente en uttømmende politiattest for å avdekke om et helsepersonell er under etterforskning. De mener at en slik hjemmel vil bidra til at Helsetilsynets arbeid med ivaretakelsen av sikkerhet og kvalitet i helsetjenesten kan fortsette.

Luftfartstilsynet[170] på sin side uttaler at de ser for seg en automatisert løsning hvor personer som innehar sertifikater innen luftfarten får sine fødselsnumre «vasket mot politiets registre» med jevne mellomrom. På denne måten kan vaskingen av fødselsnumre avdekke om noen av sertifikatinnehaverne har noe uoppgjort hos politiet eller på andre har opptrådt på en måte som er uforenlig med å inneha luftfartssertifikater. Det anser at en slik ordning vil kunne bidra til å ivareta sikkerheten innenfor luftfarten. Samtidig påpeker de at dette vil være en ressurseffektiv løsning da opplysningene kan sendes og mottas elektronisk. De påpeker avslutningsvis at opplysningene som fremkommer av denne vaskingen åpenbart må sikres mot at uvedkommende får tilgang til dem.

Arbeids- og administrasjonsdepartementet[171] presenterer generelle betraktninger angående politiattester, vandelskontroll, hvilke krav som må ligge til grunn for disse, hva som bør hjemles i lovverket og hvilken effekt politiattest som institusjon har på samfunnet. De påpeker også viktigheten av rehabiliteringsprinsippet og den dømtes behov for personvern. I dette omtaler de også utfordringer knyttet til opplysningskvalitet over tid, da en politiattest alene ikke nødvendigvis gir et riktig bilde av en persons skikkethet, da opplysningene kan være korrekte men ikke nødvendigvis gi en representasjon av dagens virkelighet.

Domstoladministrasjonen[172] uttaler at de bruker straffeattester for å kunne avklare om en tiltalt er tidligere straffedømt, og om det eventuelt skal påvirke straffeutmålingen i den aktuelle saken. De ønsker at denne ordningen skal fortsette. Samtidig bruker de vandelskontroll i de tilfeller hvor det skal ansettes nye dommere eller dommerfullmektigere. De ønsker også at denne ordningen skal fortsette som før.

---

169 Helsetilsynet, Vist, and Kristensen, NOU 2003: 21 Kriminalitetsbekjempelse og personvern.

170 Luftfartstilsynet, Sandall, and Skogstad, NOU 2003:21 Kriminalitetsbekjempelse og personvern.

171 Arbeids- og administrasjonsdepartementet, Tverfjell, and Hage, Høring - NOU 2003: 21 Kriminalitetsbekjempelse og personvern.

172 Domstolsadministrasjonen, Endresen, and Karterud, HØRINGNOU 2003: 21 KRIMINALITETSBEKJEMPELSE OG PERSONVERN.

6.2 Vandelskontroll og politiattest vs. Krav fra interesseteorien

I det følgende vil jeg anvende teori på de deler av høringsuttalelsene som omhandler vandelskontroll og politiattester. Jeg har plukket ut enkelte krav fra interesseteorien som jeg mener er relevant for mine videre analyser. De enkelte kravene vil følgelig danne underkapitlene videre i dette kapittelet.

6.2.1 Krav om opplysningskvalitet

Som utdragene fra høringsuttalelsene ovenfor viser anerkjennes det fra flere av instansene at nettopp opplysningskvalitet er viktig når det kommer til vandelskontroll og politiattester. Slik vandelskontroller og politiattester brukes kan de i mange tilfeller være tunga på vektskåla når det kommer til hvorvidt en person skal ansettes i en stilling eller ikke. Hvis opplysningene som påføres den aktuelle vandelskontrollen eller politiattesten da ikke er korrekt, relevant eller oppdatert kan det bety at denne vedkommende ikke får en jobb hen kanskje skulle hatt, var opplysningene i attesten korrekte.

Særlig Datatilsynets bemerkninger om en uttømmende politiattests innhold- og tidsbegrensning knytter seg til kravet om opplysningskvalitet. Som navnet tilsier skal en slik politiattest være uttømmende, altså alt skal påføres. Som Datatilsynet påpeker er ikke opplysningskvalitet en statisk verdi som er lik i alle år. Opplysningenes grad av validitet, eller i hvilken grad det er samsvar mellom opplysningene og virkeligheten, påvirkes ofte av tidens tann. Selv om noen har gjennomført en kriminell handling som ung betyr ikke det nødvendigvis at man er kriminell hele livet, selv om en uttømmende politiattest vil hevde dette.

Lovforslaget åpner også muligheten for å påføre verserende saker og/eller ikke-verifiserte opplysninger på en vandelskontroll/politiattest. I disse tilfellene skal det eksplisitt anmerkes på kontrollen eller attesten at opplysningene stammer fra en verserende sak eller må tolkes som ikke-verifiserte opplysninger. Begge disse kategoriene av opplysninger må kunne sies å ha en varierende grad av kvalitet og validitet.

Ett av aspektene ved kravet til opplysningskvalitet som sees ivaretatt når det kommer til vandelskontroll og politiattest er opplysningenes identifiserbarhet – altså hvorvidt de kan knyttes til den personen opplysningene er ment å beskrive. Dette ivaretas gjennom at politiattester kun kan begjæres av den som opplysningene gjelder og vedkommende må i denne anledning fremvise gyldig identifikasjon[173]. På denne måten kan politiet påføre de opplysningene som tilhører vedkommende person uten nevneverdig risiko for forveksling.

[173] Justis- og beredskapsdepartementet, "Lovvedtak 38 (2009-2010)." § 44

6.2.2 Krav om behandlingskvalitet

Hordaland Politidistrikt påpeker at tidligere praksis rundt vandelskontroller og politiattester til dels har vært preget av vilkårlighet og en betydelig grad av uoversiktlighet. Når lovforslaget nå søker å samle og tydeliggjøre lover og regler knyttet til dette anses det som positivt hos de fleste høringsinstansene. Dette kan også ha ringvirkninger når det kommer til behandlingskvaliteten, særlig for å motvirke nettopp vilkårlighet og uoversiktlighet.

Det som likevel er gjennomgående i politietatens uttalelser er frykten for et økt merarbeid knyttet til vandelskontroller og politiattester, hvor noen også mener at dette kan gå negativt utover politiets primæroppgaver. Selv om slike bemerkninger ikke har direkte tilknytning til kravet om behandlingskvalitet, legger lovforslaget opp til at saksbehandlingen knyttet til vandelskontroll og politiattest kan effektiviseres gjennom bruk av datasystemer og registre. Dette gjøres ved å uttrykkelig angi hvilke deler av lovverket som skal gjelde for den enkelte politiattest, og således kan sannsynligvis deler av saksbehandlingen langt på vei automatiseres. Dette er det likevel ingen av høringsinstansene som har fremmet i sine uttalelser, da fokuset synes å ligge på et økt ressursbehov knyttet til saksbehandlingen.

6.2.3 Krav om vern av individets identitetsbilde

Selv om høringsinstansene ikke eksplisitt nevner et krav om vern av individets identitetsbilde er det likevel relevant å se kravet i sammenheng med bruk og utstedelse av vandelskontroll og politiattester. Høringsinstansene nevner utfordringer knyttet til hvor langt tilbake i tid en skal gå for å innhente informasjon i en politiattest. Med tanke på at opplysninger om en persons livssituasjon kan endre seg over tid, kan også en politiattest inneholde misvisende opplysninger om en persons skikkethet eller egnethet til å inneha en type stilling eller arbeid. For den opplysningene gjelder kan det også oppleves belastende å bli «påminnet gamle synder» som på ingen måte representerer det mennesket vedkommende har blitt til i voksen alder.

Lovforslaget legger opp til at et vern om individets identitetsbilde når det kommer til vandelskontroller og politiattester kan ha betydning. Dette sees gjennom anledningen til å anmerke færre opplysninger på en politiattest hvis det «*ikke strider mot formålet med politiattesten og anmerkningen kan få uforholdsmessige konsekvenser for den politiattesten gjelder*[174]». Det må likevel være opp til den enkelte arbeidsgiver å vurdere opplysningene som fremkommer av en vandelskontroll eller politiattest, og videre avgjøre hvorvidt opplysningene skal eller bør ha betydning for ansettelsen.

[174] Justis- og beredskapsdepartementet. §42

6.2.4 Krav om uhindret dialog

Når det kommer til kravet om uhindret dialog i interesseteorien er det få bemerkninger angående dette fra høringsinstansene. Politietaten bemerker at den økte bruken av politiattester med påfølgende merarbeid knyttet til fornyelse av politiattester bør tilsi at det kan kreves et utstedelsesgebyr for politiattester. Ifølge interesseteorien kan et krav om vederlag eller betaling for å komme i kontakt med den behandlingsansvarlige anses som et formelt tilgjengelighetshinder. Et krav om betaling for å kunne få utstedt en politiattest må anses å falle inn under interesseteoriens beskrivelse av kravet til uhindret dialog. Politiregisterutvalget behandlet også spørsmålet om betaling for politiattester i sin utredning og kom frem til at det ikke var en ønskelig løsning.

6.2.5 Krav om rettsinformasjon

Som noen av høringsinstansene påpeker sees det som positivt at bestemmelser knyttet til vandelskontroll og politiattester er samlet i ett lovverk. Dette vil skape forutsigbarhet for den enkelte, en mulighet for den enkelte å gjøre seg kjent med bestemmelsene i lovverket samtidig som det kan motvirke vilkårlighet når det kommer til vandelskontroll og politiattest. Likeså vil et klart og tydelig lovverk motvirke krenkelser av personvernet. Dette stemmer godt overens med interesseteoriens krav om rettinsformasjon

6.3 Vektlegges kriminalitetsbekjempelsen eller personvernet?

Når det gjelder vandelskontroll og politiattester viser det seg et relativt tydelig skille mellom aktørene og hva de påpeker. Politietaten påpeker i flere høringsuttalelser at kravene til politiattest kan medføre merarbeid, økt behov for ressurser og en risiko for at politiets primæroppgaver blir lidende ved gjennomføringen av lovverket med hensyn til vandelskontroller og politiattester. Politietaten påpeker hverken aspekter knyttet til kriminalitetsbekjempelse eller til personvernet, men derimot er de opptatt av personell- og ressursbehov når det kommer til vandelskontroll og politiattester. Faktum er det at politietaten gjennomfører vandelskontroller og utsteder politiattester for andre enn seg selv – det er således en del av politietatens servicefunksjon. Det er mulig å tenke seg flere grunner til at politietaten selv vektlegger ressursbehov fremfor kriminalitetsbekjempelse eller personvern i sine uttalelser knyttet til vandelskontroll og politiattester. En kan tenke seg at politietaten anser dette temaet som så viktig at det bør legges til rette for å styrke institusjonen, som vandelskontroll og politiattest er, med ytterligere ressurser. Det kan også tenkes at politietaten ser langsiktige gevinster knyttet til kriminalitetsbekjempelsen ved å tilføre ytterlige ressurser til vandelskontroll- og politiattestinstitusjonen. Det kan også tenkes at politietaten ikke anser vandelskontroll og politiattest som et særlig viktig område og at det i mange tilfeller tar bort tid fra politiets primæroppgaver, hvorpå de «nye» ressursene kan brukes til vandelskontroll og politiattest, mens de «gamle» ressursene

kan frigjøres til å fylle politiets primæroppgaver. Jeg vet ikke hvilken, eller om noen, av disse tankene som gjenspeiler politietatens holdninger best. Jeg syns likevel det er påfallende at hverken kriminalitetsbekjempelse eller personvern vektlegges i noen særlig grad i politietatens uttalelser.

Andre, ikke-politifaglige instanser, påpeker viktigheten av at barn og unge beskyttes ved hjelp av krav om politiattester i ulike yrker som skal omgås barn og unge. Samtidig påpeker blant annet tilsynsmyndigheter at opplysninger som fremkommer i en politiattest kan være særlig sensitive og påføre store skader for den registrerte, skulle opplysningene komme på avveie.

Det fremstår som at de ikke-politifaglige instansene i større grad får frem poenger knyttet til kriminalitetsbekjempelsen og personvernet. Det ser ut til at vandelskontroll og politiattester har flere funksjoner ved seg, både når det gjelder kriminalitetsbekjempelse og personvern, og kanskje særlig gjelder dette når kriminalitet skal forebygges.

Jeg vil si at for de ikke-politifaglige instansene later det til at vektingen mellom kriminalitetsbekjempelse og personvern er relativt balansert. Det anerkjennes at det foreligger utfordringer knyttet til både kriminalitetsbekjempelsen og personvernet, men det søkes tilsynelatende å oppnå en slags balanse rundt dette når det kommer til vandelskontroll og politiattester.

Politietaten selv later til å ikke vektlegge hverken kriminalitetsbekjempelsen eller personvernet når de omtaler vandelskontroll og politiattester, men har heller et fokus på økt arbeidsmengde og behov for økte ressurser.

7 Informasjonssikkerhet/sporbarhet

God informasjonssikkerhet skal besørge konfidensialitet, integritet og tilgjengelighet. Med dette menes at informasjonssikkerhet står som et internkontrolltiltak som skal ivareta opplysningers integritet, at de ikke tilkommer uvedkommende og at de er tilgjengelige når det er nødvendig. Med ivaretagelse av opplysningenes integritet menes at informasjonen ikke skal endres, enten utilsiktet eller av uvedkommende.

Sporbarhet i elektroniske systemer er et tiltak innenfor informasjonssikkerheten som på mange måter skal ivareta dette. Sporbarhet i elektroniske systemer omhandler logging av brukeraktivitet, da særlig knyttet mot bruk av elektroniske registre. I det følgende vil jeg gjøre rede for høringsinstansenes syn på informasjonssikkerhet og sporbarhet i elektroniske systemer i lovforslaget. Jeg tar utgangspunkt i redegjørelsen av informasjonssikkerhet og sporbarhet fra kapittel 2.3.2.

7.1 Høringsinstansenes syn på informasjonssikkerhet/sporbarhet

Som både internkontrolltiltak og informasjonssikkerhetstiltak nevner flere av høringsinstansene kravet om sporbarhet i elektroniske systemer og kravet om skriftlighet i overføring av opplysninger. Flere av høringsinstansene fra politietaten omtaler sporbarhet i elektroniske systemer i mindre positive ordelag. Den mest tydelige høringsinstansen på dette området er Helgeland Politidistrikt som fremstiller kravet om sporbarhet i elektroniske systemer på følgende måte;

«F*ørst og fremst tror jeg at «trusselen» om sporbarhet vil kunne hindre en optimal kriminalitetsbekjempelse. Hvis ønsket er at alt politioperativt personell skal bidra i dette arbeidet, må det ikke legges for strenge begrensninger – selv om politimannen ikke direkte arbeider med den konkrete saken. Hvor ofte er det ikke at tjenestemenn på nattevakter eller en stille søndag formiddag har spanet i tilgjengelige registre eller lest i en aktuell straffesak, og på denne måten fått på plass brikken som mangler i puslespillet? Dette må vi fortsatt kunne gjøre uten å risikere etterfølgende etterforskning. Med sporbarhet tror jeg etaten taper mer enn den vinner.*

(...) Jeg mener bestemt at for å få best mulig resultat må «tillit» være en hovedrettesnor i hele politivesenet. Den enkelte tjenestemann må kunne tilegne seg kompetanse på egen hånd, bl.a. ved å lese aktuelle straffesaksdokumenter, eller spane i registre. Om sporbarhet til slutt vil bli resultatet, må dette kun benyttes i de tilfeller hvor det kan være snakk om at tjenestemenns

handlinger har skadet etterforskningen eller lignende ved for eksempel lekkasjer til pressen, og ikke fordi en kunnskapssøkende kollega har lest en aktuell straffesak.[175]»

Slik Helgeland Politidistrikt uttaler seg er det tydelig en misnøye å spore når det kommer til sporbarhet i elektroniske systemer. De gjør det klart at de ønsker en «tillitsbasert kultur» fremfor risikoen for å bli tatt i å «snoke i registre». De bruker også politioperative argumenter for hvorfor sporbarhet i elektroniske systemer ikke burde gjennomføres. Fokuset for Helgeland Politidistrikt synes å være på «optimal kriminalitetsbekjempelse» fremfor godt personvern og sikre datasystemer. Jeg opplever det slik at politidistriktet mener at sporbarhet i elektroniske systemer utelukkende er til for å ta de som snoker i politiets registre, og at det i større grad burde foreligge en slags tillitskultur, fremfor overvåking av polititjenestemenn. I alle hovedsak er det likevel slik at sporbarhet i elektroniske systemer langt på vei er et tiltak for å ivareta personvernprinsipper, besørge trygge datasystemer og avdekke uautorisert bruk av politiets registre.

Politiets Data- og Materielltjeneste (PDMT) omtaler også sporbarhet i elektroniske systemer i sin høringsuttalelse[176]. De presenterer sine synspunkter fra en mer systemteknisk side og bemerker at logging vedrørende brukeraktiviteter, på høringstidspunktet, er implementert i systemene i varierende grad, blant annet på grunn av systemenes ytelsesnivå. De mener at for å fullt utfylle lovens krav om sporbarhet i elektroniske systemer er ny arkitektur og nye systemer en forutsetning. De påpeker også at innføring av sporbarhet i den systemporteføljen som foreligger vil medføre svært store kostnader.

PDMT anser også at lagringstiden på logger à 3 måneder er for kort og at en lengre lagringstid bør plasseres i forskriften.

Romerike Politidistrikt på sin side opplever at *«forslag om (...) internkontroll, informasjonssikkerhet og sporbarhet anses (...) som en kodifisering av gjeldende praksis, som ikke får vesentlig praktisk betydning for politidistriktet.[177]»*

Rogaland Politidistrikt[178] bemerker at forslagene knyttet til meldeplikt, internkontroll, informasjonssikkerhet og sporbarhet medfører økt behov for ressurser.

Kriminalpolitisentralen (KRIPOS)[179] bemerker at skriftlighet når det kommer til utlevering av opplysninger til tredjeparter (eksempelvis Tollvesenet) er med på å sikre notoritetshensyn,

---

175 Helgeland politidistrikt and Fjærli, Høring - NOU 2003:21 Kriminalitetsbekjempelse og personvern.

176 Politiets Data- og Materielltjeneste (PDMT) and Bøhler, Kriminalitetsbekjempelse og personvern - Høring.

177 Romerike politidistrikt and Plathe Maartmann, Høring - NOU 2003:21 - Kriminalitetsbekjempelse og personvern - politiets og påtalemyndighetes behandling av opplysninger.

178 Rogaland politidistrikt, Sønderland, and Andersen, NOU 2003:21 - Kriminalitetsbekjempelse og personvern - politiets og påtalemyndighetes behandling av opplysninger - Høring.

179 Kriminalpolitisentralen (KRIPOS), Frigaard, and Wiese Bromander, Høringsuttalelse - NOU 2003:21 - Kriminalitetsbekjempelse og personvern - politiets og påtalemyndighetes behandling av opplysninger.

men at det likevel bør tilføyes unntak fra kravet til skriftlighet. Dette begrunnes i et relativt dynamisk samarbeid mellom politietaten og Tollvesenet som ikke alltid legger til rette for skriftlighet i utlevering av opplysninger.

KRIPOS legger vekt på at ikke-verifisert informasjon må tydeliggjøres som nettopp dette i de tilfeller hvor slik informasjon utleveres. De mener videre at nedtegning av utlevering av opplysninger til parter som er underlagt taushetsplikt, fremstår som unødvendig og upraktisk, og at et unntak formuleres slik at varslingsplikten ikke utløses.

KRIPOS poengterer videre at kravene som lovverket nedsetter forutsetter betydelige oppdateringer av datasystemene som omfattes av Politiregisterloven.

Østfold Politidistrikt[180] bemerker det samme som KRIPOS i at skriftlighet fremstår som delvis positivt med hensyn til personvern og rettssikkerhet og delvis negativt da det er vanskelig gjennomførbart i visse situasjoner, i tillegg til å være arbeidskrevende for politiet.

Datatilsynet[181] ytrer i sin høringsuttalelse at sporbarhet i elektroniske systemer og logging av brukeraktivitet er særdeles viktig for å kunne ivareta de registrertes personvern, samt å føre kontroll med at de som bruker de elektroniske registrene har tjenstlig behov for å ha tilgang til opplysningene i registrene. Tilsynet påpeker samtidig at polititjenestemennene som bruker registrene og får sin brukeraktivitet logget får sitt eget personvern truet. De legger således vekt på at overvåkingen og bruken av logger kun brukes for å føre kontroll med tilgangsrettigheter og intern sikkerhet.

Skattedirektoratet[182] påpeker at det er viktig at det både subjektivt og objektivt oppleves en tilstrekkelig grad av oppdagelsesrisiko. Med dette menes at uautorisert bruk og tilgang til konfidensielle opplysninger oftest foregår i det skjulte, og de personene som opplysningene gjelder får aldri vite at deres opplysninger er på avveie. Således må det foreligge løsninger som sørger for at uautorisert tilgang til opplysninger oppdages tidlig og håndteres deretter. Er sjansen stor for å bli oppdaget som en som snoker i registre, vil det etter all sannsynlighet være slik at snokeren avstår fra å benytte en uautorisert tilgang.

Skattedirektoratet[183] påpeker videre at informasjonsutveksling mellom offentlige etater sees som positivt særlig med tanke på kriminalitetsbekjempelsen. Like fullt må en slik informasjonsutveksling baseres på «tjenstlig behov» - altså ikke hvem som helst kan få tilgang til

[180] Østfold politidistrikt, Lien, and Arnesen, Høring - NOU 2003:21 - Kriminalitetsbekjempelse og personvern.

[181] Datatilsynet, Apenes, and Gulbrandsen, HØRINGSUTTALELSE.NOU 2003:21 KRLMINALITETSBEKJEMPELSE OG PERSONVERN.

[182] Skattedirektoratet, Nilsen, and Grini, Høring - NOU 2003:21 - Om Kriminalitetsbekjempelse og personvern.

[183] Skattedirektoratet, Nilsen, and Grini.

informasjonen som utveksles, det må finnes et behov som ligner på kriteriene nedsatt i Personopplysningsloven §§ 8 og 9[184]. Med dette menes at de som får tilgang til opplysninger må ha et behov for å ha denne tilgangen, som oftest basert på et behov for å utøve offentlig myndighet, oppfylle en rettslig forpliktelse eller lignende. Videre anser Skattedirektoratet utfordringer knyttet til informasjonsutveksling og personvern. Dette kan videre løses med streng tilgangskontroll, basert på nettopp tjenstlig behov.

Nærings- og handelsdepartementet[185] påpeker viktigheten av autentisering av opplysninger – videre forklart som *«at det skal være tydelig hvem som har innført opplysningen i angjeldende system[186]».* Departementet mener videre at elektroniske signaturer, basert på «Public Key Infrastructure»-teknologi[187], vil bidra både til autentisering og et bedre personvern gjennom integritetssikring. I tillegg kan bruk av elektronisk signatur langt på vei erstatte tradisjonell logging av systembruk, da elektroniske signaturer er sporbare og i mindre grad er inngripende ovenfor de ansattes personvern.

Nasjonal Sikkerhetsmyndighet[188] (NSM) bemerker på sin side forholdet til PST og deres behandling av opplysninger med hjemmel i Sikkerhetsloven. NSM mener at det vil være riktig å henvise til Sikkerhetsloven i Politiregisterlovens paragrafer om informasjonssikkerhet, da Sikkerhetslovens bestemmelser medfører strengere krav til informasjonssikkerhet enn Politiregisterlovens bestemmelser.

Juss-Buss[189] stiller seg positive til kravet om skriftlighet når det gjelder overføring av opplysninger, og i deres høringsuttalelse, særlig for overføring av opplysninger fra politiet til fengselsvesenet. Ifølge Juss Buss vil et slikt krav motvirke «kompis-tonen» som kan oppstå mellom politiet og fengselsvesenet hvis opplysninger skal kunne overføres muntlig.

Den Norske Advokatforening (DNA)[190] stiller seg positive til lovforslaget og bemerker at *«Når det gjelder (...) kravene til informasjonssikkerhet, internkontroll og sporbarhet styrker dette kravene til korrekt bruk av opplysningene, samt bidrar til at opplysningene ikke benyttes til andre formål eller kommer uvedkommende i hende.»*

---

184 Justis- og beredskapsdepartementet, "popplyl." §8 bokstav b og e, samt §9 bokstav f

185 Nærings- og handelsdepartementet, Bjørke, and Norum R., NOU 2003:21 Kriminalitetsbekjempelse og personvern - Høringsuttalelse.

186 Nærings- og handelsdepartementet, Bjørke, and Norum R. Femte avsnitt

187 Direktoratet for forvaltning og IKT, "PKI."

188 Nasjonal Sikkerhetsmyndighet and Larsen, Horing - NOU 2003: 21 Kriminalitetsbekjempelse og personvern.

189 Juss-Buss, Siljan, and Lehmann, Høringssuttalelse - NOU 2003:21 Kriminalitetsbekjempelse og personvern.

190 Den Norske Advokatforening, Aarseth, and Smith, Høringssuttalelse - NOU 2003:21 Kriminalitetsbekjempelse og personvern.

7.2 Informasjonssikkerhet/sporbarhet vs. Krav fra interesseteorien

I det følgende vil jeg anvende teori på de delene av høringsuttalelsene som omhandler internkontroll/informasjonssikkerhet. Høringsuttalelsene viser at høringsinstansene var særlig opptatt av sporbarhet i elektroniske systemer, og jeg vil følgelig bruke deler av interesseteorien for å se nærmere på nettopp dette. Jeg har plukket ut enkelte krav fra interesseteorien som jeg mener er relevante for å kunne analysere høringsinstansenes syn på internkontroll og informasjonssikkerhet. De enkelte kravene vil videre utgjøre delkapitler i mine vurderinger.

7.2.1 Kravet om forholdsmessighet mellom ekstern og intern kontroll

Sporbarhet i elektroniske systemer eller logging av brukeraktivitet i politiregistre er et internkontrolltiltak, såvel som et informasjonssikkerhetstiltak. Høringsinstansene bemerker både tilfredshet og misnøye med innføringen av en intern kontroll eller overvåkning av politiets bruk av elektroniske systemer. Alternativet til innføringen av sporbarhet i elektroniske systemer kan være at den registrerte selv kan gjennomføre kontrollen gjennom en utvidet innsyns- og klagerett. Ifølge interesseteorien er det nettopp en forholdsmessighetsvurdering som skal gjennomføres når det kommer til innføringen av interne- eller eksterne kontrolltiltak. I dette ligger det at den registrerte selv ikke skal måtte stå ansvarlig for at den behandlingsansvarlige følger gjeldende lovverk knyttet til behandling av opplysninger. Hvis en skal utvide kontrolltiltak mot den registrerte eller begrense den registrertes mulighet til å føre kontroll, må det også tas med i vurderingen om den interne kontrollen er tilfredsstillende nok. En søker således å oppnå en god balanse mellom ekstern- og intern kontroll.

Helgeland Politidistrikt uttaler tydelig i sitt høringssvar at de ikke verdsetter sporbarhet i elektroniske systemer og den trusselen det utgjør mot de ansatte. De hevder videre at et slikt kontrolltiltak kan eller vil skade politiets primæroppgaver og at den enkelte polititjenestemann ikke skal straffes for å være kunnskapssøkende i politiarbeidet. De opplever således at kontrolltiltaket er en form for unødvendig overvåkning, og at de registrerte heller bør ha tillit til at politiet foretar sitt arbeid i tråd med gjeldende regelverk.

Datatilsynet på sin side anser også at den interne kontrollen kan medføre utfordringer knyttet til de ansattes personvern, men at kontrollen bør begrenses til de tilfeller hvor det er ment å avdekke straffbare forhold, som brudd på tilgangsrettigheter mv. De anser således ikke den interne kontrollen å være i motstrid med forholdsmessigheten mellom intern- og ekstern kontroll.

7.2.2 Kravet om forholdsmessighet mellom kontroll til de registrertes gunst og til deres ugunst

Datatilsynet bemerker i sin høringsuttalelse at sporbarhet i elektroniske systemer er et viktig verktøy i kontrollen av de registrertes personvern. Likeså ser de viktigheten av at polititjenestemennenes eget personvern ivaretas når et slikt kontrolltiltak skal benyttes. En kan således si at det finnes to grupper av «registrerte»; de som har opplysninger om seg selv lagret i politiets elektroniske systemer og polititjenestemennene selv. Datatilsynet påpeker derfor et viktig poeng, nettopp at bruken av logging kun brukes i de tilfeller hvor kravene til sikkerhet og tilgang skal kontrolleres. Med andre ord mener Datatilsynet at sporbarhet i elektroniske systemer ikke skal være en slags overvåkning av den enkelte polititjenestemann, men et verktøy for å ivareta den interne sikkerheten i systemene og avdekke eventuelle brudd på tilgangen den enkelte polititjenestemann har. Dette argumentet føyer seg inn i rekken av argumenter, særlig fra Helgeland Politidistrikt som mener at et slikt kontrolltiltak kan benyttes til å straffe eller kontrollere polititjenestemenn, fremfor å avdekke alvorlige brudd på sikkerheten mv.

Noen få andre høringsinstanser bemerker at skriftlighet i overføring av opplysninger kan føre til bedre notoritet på opplysningene, ivaretakelse av personvernet og den registrertes rettigheter. Dette gjelder blant annet JussBuss som påpeker at forholdet mellom politi og fengselsvesen ofte er preget av muntlig overføring av opplysninger, noe som kan påvirke de innsattes situasjon negativt. Ved å kreve skriftlighet i overføring av opplysninger kan en se sammenhengen med kravet om forholdsmessighet mellom kontroll til de registrertes gunst og til deres ugunst. Skriftlighet i overføring av opplysninger kan sees som et kontrolltiltak som er til de registrertes gunst, samtidig som tiltaket kan bedre den behandlingsansvarliges mulighet til å føre kontroll med opplysninger som forlater den behandlingsansvarliges kontroll.

KRIPOS påpeker noe av det samme i sin høringsuttalelse, hvor de anerkjenner at skriftlighet i overføring av opplysninger skaper notoritet, mens det på samme tid oppleves tungvint i gitte situasjoner. De fremstår således noe mer delt i sin oppfatning, sammenlignet med JussBuss.

Ifølge interesseteorien skal en tilstrebe å føre kontroll til de registrertes gunst, og ikke til deres ugunst. I dette tilfellet gjelder det for begge gruppene av «registrerte». Sporbarhet i elektroniske systemer sees som viktig for å ivareta den enkeltes personvern og som et verktøy for å besørge god sikkerhet og tilgangskontroll i systemene. Som både Datatilsynet og politidistriktet påpeker må det foreligge en forholdsmessighetsvurdering rundt innføringen av sporbarhet i elektroniske systemer og rundt hvorvidt kontrollen er til de registrertes gunst eller ugunst.

7.2.3 Krav om behandlingskvalitet

Når det kommer til kravet om behandlingskvalitet påpeker noen av høringsinstansene at kravet om skriftlighet i overføring av opplysninger fremstår som tungvint og til dels vanskelig gjennomførbart. Når opplysninger som politiet eller påtalemyndigheten innehar skal utleveres til andre legger Politiregisterloven føringer på at opplysningene skal overføres skriftlig, fremfor muntlig. Hensikten med dette er å skape notoritet – altså en mulighet for den behandlingsansvarlige å ha kontroll med hvilke opplysninger som utleveres, til hvem de utleveres mv. Skulle det da forekomme at de utleverte opplysningene kommer på avveie eller blir brukt av uvedkommende kan den behandlingsansvarlige gå tilbake i det skriftlige materialet for å avgjøre hvem som eventuelt skal stilles til ansvar og hvorvidt lovverket er overholdt.

Særlig politietaten, blant annet gjennom KRIPOS, påpeker at skriftlighet i overføring av opplysninger ofte kan fremstå tungvint og kan forhindre et effektivt samarbeid mellom politiet og andre aktører. KRIPOS trekker frem Tollvesenet som eksempel, da de i relativt stor grad har et samarbeid om å føre kontroll med varer som kommer inn til Norge. Som KRIPOS selv påpeker er dette samarbeidet preget av å foregå i korte tidsperioder, eksempelvis en kontroll av et kjøretøy på Svinesund. Hvis da Tollvesenet ønsker opplysninger fra Politiet om fører av kjøretøyet eller lignende må de kontakte Politiet, som videre kan avgi opplysninger til Tollvesenet. Siden Politiregisterloven krever at slik utlevering av opplysninger skal skje skriftlig, blir Tollvesenet satt i en situasjon hvor de må vente på skriftlig utlevering av opplysninger, fremfor at Politiet kan avgi denne informasjonen muntlig. Politiregisterutvalget uttaler at skriftlighet er ønskelig for å ivareta notoritet, men at det i et fåtall saker kan fravikes kravet om skriftlighet.

Juss-Buss uttaler i sitt høringssvar at skriftlighet ved utlevering av opplysninger oppleves som særlig positivt da det «motvirker kompis-tonen» som de mener kan forekomme mellom politiet og fengselsvesenet. De påpeker således også et ønske om økt notoritet på de opplysningene som utleveres fra politiet til fengselsvesenet med tanke på de innsattes rettigheter og personvern.

7.2.4 Krav om konfidensialitet

Internkontroll- og informasjonssikkerhetstiltak er blant annet ment å ivareta konfidensialiteten når det kommer til behandling av opplysninger. For politiet og påtalemyndigheten er konfidensialitet særdeles viktig da de behandler store mengder sensitiv personinformasjon og skulle slik informasjon komme på avveie kan det få alvorlige følger. Sporbarhet i elektroniske systemer er også et verktøy for å ivareta konfidensialiteten. Nettopp ved å kunne føre kontroll med hvem som gjør seg kjent med ulike typer informasjon, kan en også «følge brødsmulene»

tilbake hvis opplysninger skulle komme på avveie. Skattedirektoratet påpeker at sporbarhet i elektroniske systemer har en forebyggende effekt og at oppdagelsesrisikoen bør være tilstrekkelig høy nok til at misbruk av opplysninger ikke lett skal finne sted. Slik sett må en kunne si at sporbarhet i elektroniske systemer kan bidra til å ivareta konfidensialitetsprinsipper innenfor politi og påtalemyndighet.

7.2.5 Krav om etablert tillitsforhold

Siden kravet om etablert tillitsforhold hovedsaklig baserer seg på tilfeller hvor behandlingen av personopplysninger er basert på samtykke, eller av en annen grunn ønsket av den registrerte, passer dette dårlig med politiets behandling av opplysninger som hovedsaklig har et annet rettslig grunnlag. I mange tilfeller vet ikke den registrerte at politiet eller påtalemyndigheten behandler opplysninger om hen, da dette kan forringe kriminalitetsbekjempelsen og politiarbeidet forøvrig. Likevel burde politiet i sin maktposisjon være en etat som folk flest har tilitt til. Dette påpekes også av Helgeland Politidistrikt som tydelig ytrer i sin høringsuttalelse at sporbarhet i elektroniske systemer kan medføre et større tap enn gevinst for etaten. Distriktet påpeker at det etablerte tillitsforholdet bør være en rettesnor i behandlingen av opplysninger, fremfor at politietaten skal overvåkes gjennom logging av brukeraktivitet i politiets registre.

Siden flere av sikkerhetsventilene som skal ivareta de registrertes interesser er strupet eller tatt bort, kan det vanskelig sies at den registrerte skal ha uforbeholden tillit til at politiet behandler opplysninger om dem i tråd med lovverket. Med dette må innføringen av andre kontrolltiltak sees som nødvendige for å ivareta de registrertes personvern.

En kan argumentere for at sporbarhet i elektroniske systemer og informasjonssikkerhet på generell basis kan bidra til å øke tilliten befolkningen har til politietaten. På bakgrunn av mine egne følelser knyttet til dette vil jeg anta at mange vil oppleve en økt trygghet i det at enhver polititjenestemanns brukeraktivitet på elektroniske systemer bli loggført og kan bli overvåket. En trenger således ikke være redd for at naboen som jobber i politiet skal ta seg friheter og snoke i registre for å eksempelvis kunne ha et overtak i en privatrettslig nabodisputt. For befolkningen sin del vil jeg også anta at vissheten om at politietaten har lover og regler de må etterleve når det kommer til behandling av opplysninger må oppleves tryggende og tillitsskapende. Under forutsetning om at sporbarhet i elektroniske systemer benyttes slik det er tiltenkt, mener jeg at dette, sammen med god informasjonssikkerhet og internkontroll, vil skape økt tillit til politietaten.

7.3 Vektlegges kriminalitetsbekjempelsen eller personvernet?

Ovenfor har jeg gjort rede for hva informasjonssikkerhet og sporbarhet i elektroniske systemer innebærer, samt hva høringsinstansenes syn på dette var i forhold til lovforslaget. I det

følgende skal jeg drøfte hvorvidt det er kriminalitetsbekjempelsen eller personvernet som vektlegges i høringsinstansenes diskusjoner.

Sporbarhet i elektroniske systemer, eller logging av brukeraktivitet i politiets registre, er et tiltak som har flere hensikter. Det er for det første ment som et verktøy for å ha kontroll på de opplysningene som politiet besitter. For det andre er det ment som et verktøy for å avdekke uautorisert bruk eller tilgang på opplysninger blant polititjenestemenn eller andre med tilgang til politiets registre. For det tredje skal de bidra til å opprettholde opplysningenes konfidensialitet og opplysningenes integritet. For det fjerde kan sporbarheten bidra til at befolkningen får en økt tillit til politietaten og hvordan politietaten behandler opplysninger. Til slutt kan sporbarhet i elektroniske systemer i politiet medføre at polititjenestemennene selv blir seg selv og sitt samfunnsansvar mer bevisst. Med dette menes at det forventes at politiet, som håndhever av loven, overholder lovverket selv. Det faktum at brukeraktivitet logges bør bidra til at snoking i registre, eller naboens gjøren og laden, ikke blir så interessant med fare for sanksjoner i etterkant.

Interesseteoriens krav om forholdsmessighet i kontrolltiltak står særdeles sentralt i denne diskusjonen. Er innføringen av sporbarhet i elektroniske systemer et kontrolltiltak som står i forhold til alternativet om å ikke innføre kontrolltiltak? Og er kontrolltiltaket til de registrertes gunst eller til deres ugunst? Det er for meg liten tvil om at dette handler om personvern og ikke om kriminalitetsbekjempelsen. Tiltakets ulike hensikter, som beskrevet ovenfor, understøtter min opplevelse av tiltakets mål om å ivareta personvernet. Slik sporbarheten er tiltenkt som et kontrolltiltak, står det også i forholdsmessighet til alternativet om å ikke innføre kontrolltiltak, eller innføre kontrolltiltak som hovedsaklig er eksternt, fremfor internt.

Om tiltaket med sporbarhet i elektroniske systemer kan ha ringvirkninger på kriminalitetsbekjempelsen, omtales i mindre grad av høringsinstansene. Jeg kan vanskelig hevde at det har faktiske kriminalitetsbekjempende egenskaper som tiltak, men jeg kan argumentere for at tiltaket med sporbarhet kan virke kriminalitetsforebyggende. Dette handler om at sporbarheten er med på ivareta konfidensialitet og taushetsplikt, som videre er straffbart om brytes. Tiltaket sørger også for at det blir vanskeligere for uærlige polititjenestemenn å spre opplysninger til kriminelle miljøer eller skaffe seg et overtak i en eller annen privat disputt.

Det er likevel slik at personvern later til å vektlegges mest når det kommer til sporbarhet og informasjonssikkerhet.

8 Oppsummering og funn

Med utgangspunkt i NOU 2003:21 og høringsuttalelsene fra høringen av utredningen har jeg nå forsøkt å belyse hvordan forholdet mellom kriminalitetsbekjempelse og personvern var forsøkt ivaretatt i utformingen av Politiregisterloven. I tillegg til dette har jeg belyst hva høringsinstansene mente om Pool-ordningen, vandelskontroll/politiattester og informasjonssikkerhet/sporbarhet, og hvordan disse delene av det nye lovverket står seg opp mot interesseteorien.

Ut ifra min gjennomgang av høringsinstansenes svar har jeg sett at det forekommer flere ulike meninger knyttet til både kriminalitetsbekjempelse og personvern. Særlig er det tydelig for meg at politiet og påtalemyndigheten selv ønsker å ha så frie tøyler som mulig for å kunne utføre sitt viktigste arbeid – bekjempelse av kriminalitet. Med dette mener jeg at politiet og påtalemyndigheten tilsynelatende ønsker å behandle mest mulig informasjon om flest mulig personer, og merarbeid med informasjonssikkerhet og vandelskontroll sees til dels som et hinder for å utføre effektivt politiarbeid. På den andre siden hevder andre høringsinstanser at kriminalitetsbekjempelsen har trumfet personvernet og således fått altfor stor plass i lovverket. Det finnes likevel høringsinstanser som bemerker at personvernet er godt eller tilstrekkelig ivaretatt i Politiregisterloven.

Med utgangspunkt i interesseteorien er det noen av kravene som ikke lar seg anvende på deler av politiets arbeid og kriminalitetsbekjempelsen. Med dette mener jeg at deler av interesseteorien rett og slett står i så stor motsetning til kriminalitetsbekjempelsen at de ikke er mulig å se for seg ivaretatt, uten at kriminalitetsbekjempelsen blir altfor skadelidende. Dette gjelder særlig interessen i innsyn og kunnskap[191]. Med dette menes eksempelvis at interessen i innsyn og kunnskap legger opp til at enhver skal ha både generelt og individuelt innsyn i sine egne personopplysninger. For politiets del vil dette vanskeliggjøre kriminalitetsbekjempelsen, da mistenkte eller kriminelle kan få innsyn i opplysninger som er avgjørende for kriminalitetsbekjempelsen. På denne måten kan mistenkte eller kriminelle tilpasse sin atferd eller forklaring på bakgrunn av hva politiet har av opplysninger. I slike tilfeller må personvernet vike til fordel for kriminalitetsbekjempelsen. Dette bekreftes til dels av at høringsinstansene selv ikke omtaler interessen i innsyn og kunnskap.

På den andre siden er det deler av interesseteorien som må ansees som viktig at ivaretas i kombinasjon med kriminalitetsbekjempelsen. Dette gjelder hovedsaklig kravet om opplys-

[191] de Hert and Papakonstantinou, "The New Police and Criminal Justice Data Protection Directive." Kapittel 6, første avsnitt

ningskvalitet og behandlingskvalitet. Når politiet og påtalemyndigheten kan fokusere på å fremskaffe opplysninger med god kvalitet, samt at behandlingen av disse opplysningene foregår med bakgrunn i gitte rutiner og bestemmelser, kan fokuset på det som er personvern-prinsipper medføre positive ringvirkninger for kriminalitetsbekjempelsen.

Etter hva jeg kan se er det få av høringsinstansene som har fått sine bemerkninger hensyntatt i den endelige utformingen av loven. Hovedsaklig er forskjellene fra lovforslaget i NOU 2003:21 til Lovvedtak 38 (2009-2010) basert på rent språklige endringer og tydeligere syntaks. Av det jeg har kunnet se er det to deler av lovforslaget som er endret eller lagt til som følge av høringsinstansenes bemerkninger;

- Politiets Data og Materielltjeneste (PDMT) har fått gehør for sin bemerkning om lengre lagringstid av brukslogger i politiets datasystemer, fra 3 måneder til 1 år. Endringene kan sees i lovforslaget fra NOU 2003:21 i § 12 siste ledd til Lovvedtak 38 (2009-2010) § 17 siste ledd. I tillegg har Lovvedtak 38 (2009-2010) lagt til slettefrist på senest 3 år.
- I Lovvedtak 38 (2009-2010) er det tillagt en paragraf som ikke foreligger i NOU 2003:21, nemlig §39[192] om politiattest for personer som skal ha omsorg for eller oppgaver knyttet til mindreårige (barneomsorgsattest). Jeg vil anta at denne bestemmelsen kom til som en følge av hva flere høringsinstanser merket seg rundt viktigheten av å sikre barn og ungdom i barnehage, skole, barnevern og fritidsaktiviteter.

Utover dette, og hva jeg har lest av dokumentasjon, er det svært få av høringsinstansene som har fått gehør for sine bemerkninger angående lovforslaget. Hva som er grunnene til dette kan være mange. En sannsynlig grunn er at norsk lovverk i stor grad er styrt av hva slags lovverk som vedtas i EU. Parallelt med utformingen av Politiregisterloven i Norge arbeidet EU-rådet[193] med en rammebeslutning[194] som lovgiver tidlig forstod at ville medføre konsekvenser for, og endringer i, Politiregisterloven. Med tanke på at høringen til NOU 2003:21 foregikk i 2004, mens EU-rådets rammebeslutning kom til i 2008, er det ikke umulig at EU-rådets arbeid ble mer førende for utformingen av Politiregisterloven i Norge, enn hva høringsinstansens merknader ble. I tillegg til at rammebeslutningen er av nyere dato enn høringsuttalelsene, veier nok EU-rådets beslutninger betraktelig mer i det politiske landskapet.

192 Justis- og beredskapsdepartementet, "Lovvedtak 38 (2009-2010)." § 39

193 Europaportalen, "Hva er Rådet for den europeiske union?"

194 Rådet for den europeiske union, "Rammebeslutning 2008/977/JIS."

En annen sannsynlig grunn er at lovgiver har opplevd seg selv som rause mot politietaten, at de har gitt politietaten så mye spillerom som mulig i et lovforslag – og kanskje var planen å stramme inn spillerommet på sikt? Det er ihvertfall ikke utenkelig at lovgiver har måttet sette en øvre grense for hvor stort spillerom politiet og påtalemyndigheten skulle få i Politiregisterloven. Det er videre et faktum at svært få av politidistriktene eller særorganene har fått gehør for sine synspunkter etter høringsrunden, og kanskje var den øvre grensen nådd allerede før høringsrunden.

Etter å ha analysert høringsinstansenes svar til NOU 2003:21 og vurdert dem opp mot personvernteori er det klart for meg at de ulike høringsinstansene er delt i sitt syn på hvordan vektingen mellom personvern og kriminalitetsbekjempelse skal best ivaretas. Jeg ser et relativt klart skille mellom politietaten på den ene siden og de andre høringsinstansene på den andre. Politietaten selv ønsker så vide rammer for sin behandling av personopplysninger som mulig, med grunnlag i politiets kjernevirksomhet. De fremmer stadig i sine høringsuttalelser henvisninger til kriminalitetsbekjempelse, ordenstjeneste og andre politirelaterte argumenter, mens personvernet får noe mindre plass i deres uttalelser. En av høringsinstansene omtaler også et ønske om en tillitskultur, fremfor bruk av interne kontrolltiltak.

På den andre siden fremmer flere høringsinstanser krav om mer fokus på personvern, blant annet Datatilsynet og Skattedirektoratet med flere. De høringsinstansene som ikke tilhører politietaten opplever jeg at presenterer en mer balansert tilnærming til forholdet mellom kriminalitetsbekjempelse og personvern. Flere anerkjenner at politiet og påtalemyndigheten har behov for visse verktøy for å ivareta sin kjernevirksomhet, mens det samtidig påpekes at det er viktig at personvernet får sin plass i Politiregisterloven og politiets virksomhet.

Det er nok likevel slik at balansen mellom kriminalitetsbekjempelse og personvern alltid vil være å bevege seg på en knivsegg. Som mine redegjørelser viser er det flere av personvernprinsippene, eller interessene fra interesseteorien, som ikke lar seg anvende på kriminalitetsbekjempelsen[195]. Hvis vi ønsker oss et samfunn som er preget av sterke borgerrettigheter og liten grad av kriminalitetsbekjempelse, er det mulig å oppnå hvis lovverket legger opp til en slik vekting. Det er nok uansett slik at de fleste ønsker seg et minimum av kriminalitet, og et så godt personvern som mulig – uten at dette går ut over kriminalitetsbekjempelsen.

På den andre siden er det deler av interesseteorien som utvilsomt kan bidra til bedre kriminalitetsbekjempelse, uten at personvernet blir altfor lidende. Et økt fokus på opplysnings- og behandlingskvalitet, samt kontrolltiltak og informasjonssikkerhet kan bringe med

[195] de Hert and Papakonstantinou, "The New Police and Criminal Justice Data Protection Directive." Kapittel 2, fjerde avsnitt

seg positive effekter på kriminalitetsbekjempelsen – samtidig som det er personvernmessige gevinster knyttet til dette.

Litteraturliste

Lover

Justis- og beredskapsdepartementet. «Forvaltningsloven», 10. februar 1967. https://lovdata.no/pro/#document/NL/lov/1967-02-10

———. «Grunnlova - Grl.» Lovdata.no, 17.mai 1814. https://lovdata.no/pro/#document/NL/lov/1814-05-17-nn

———. «Lov om Norsk Lovtidend», 19. juni 1969. https://lovdata.no/pro/#document/NL/lov/1969-06-19-53?searchResultContext=2284

———. «Lovvedtak 38 (2009-2010) Lov om behandling av opplysninger i politiet og påtale-myndigheten (politiregisterloven)». Lovdata.no, 4. mars 2010. https://lovdata.no/pro/#document/LOVVED/forarbeid/lovvedtak-38-200910

———. «Menneskerettsloven». Lovdata.no, 21. mai 1999. https://lovdata.no/pro/#document/NL/lov/1999-05-21-30

———. «Offentleglova», 19. mai 2006. https://lovdata.no/pro/#document/NL/lov/2006-05-19-16?searchResultContext=953

———. «Personopplysningsloven», 14. april 2000. https://lovdata.no/pro/#document/NL/lov/2000-04-14-31

———. «Politiloven», 10. januar 1995. https://lovdata.no/pro/#document/NL/lov/1995-08-04-53?searchResultContext=2085

———. «Politiregisterforskriften», 20. september 2013. https://lovdata.no/pro/#document/SF/forskrift/2013-09-20-1097

———. «Politiregisterloven», 28. mai 2010. https://lovdata.no/pro/#document/NL/lov/2010-05-28-16

———. «Straffeprosessloven». Lovdata.no, 1. januar 1986. https://lovdata.no/pro/#document/NL/lov/1981-05-22-25

———. «Strafferegistreringsloven.», 11. juni 1971.
https://lovdata.no/pro/#document/NLO/lov/1971-06-11-52?searchResultContext=963

Landbruks- og Matdepartementet. «Fjellova». Lovdata.no, 6. juni 1975.
https://lovdata.no/pro/#document/NL/lov/1975-06-06-31

Bok

Bing, Jon. *Personvern i faresonen*. Brennpunkt. Oslo: Cappelen, 1991.
http://urn.nb.no/URN:NBN:no-nb_digibok_2007112304009

Bruce, Ingvild. «Personvern, rettssikkerhet og vern mot alvorlig kriminalitet - Noen utgangspunkter». I *Overvåking i en rettsstat*, 388 (62-83). Fagbokforlaget Vigmostad & Bjørke AS, 2010.

Schartum, Dag Wiese, red. *Overvåking i en rettsstat*. Bergen: Fagbokforlaget, 2010.

Schartum, Dag Wiese, og Lee A. Bygrave. *Personvern i informasjonssamfunnet: en innføring i vern av personopplysninger*. 3.utgave. Bergen: Fagbokforlaget, 2016.

Selmer, Knut S., og Ragnar Dag Blekeli. *Data og personvern*. Bd. 6. Scandinavian university books. Oslo: Universitetsforlaget, 1977.
http://urn.nb.no/URN:NBN:no-nb_digibok_2014031706032

NOU'er

Boe-utvalget. «Pseudonyme helseregistre». Regjeringen.no, 8. juli 1993.
https://www.regjeringen.no/globalassets/upload/kilde/odn/tmp/2002/0034/ddd/pdfv/154820-nou1993-22.pdf

Justis- og politidepartementet, JD. «NOU 2003:21 Kriminalitetsbekjempelse og personvern». Lovdata.no, 28. august 2003.
https://lovdata.no/pro/#document/NOU/forarbeid/nou-2003-21

Stortingsmeldinger, Odelstingsproposisjoner mv.

Justis- og beredskapsdepartementet. «St.meld. nr. 42 (2004-2005) - Politiets rolle og oppgaver». Åpnet 7. juni 2017.
https://www.regjeringen.no/no/dokumenter/stmeld-nr-42-2004-2005-/id199239/?q=politiregisterloven

Justis- og politidepartementet. «Ot.prp.nr.92 (1998-1999) Om lov om behandling av personopplysninger», 25. juni 1999.
https://lovdata.no/pro/#document/PROP/forarbeid/otprp-92-199899

———. «Ot.prp.nr.108 (2008-2009) Om lov om behandling av opplysninger i politiet og påtalemyndigheten», 21. august 2009.
https://lovdata.no/pro/#document/PROP/forarbeid/otprp-108-200809

Justis-og politidepartementet. «St.meld. nr. 22 (2000-2001)». Stortingsmelding. 012001-040010, 12. januar 2001.
https://www.regjeringen.no/no/dokumenter/stmeld-nr-22-2000-2001-/id431872/

Utenriksdepartementet. «Om samtykke til godtakelse av rammebeslutning 2008/977/JIS om personvern i forbindelse med politi- og strafferettssamarbeid». Regjeringen.no. Åpnet 6. juni 2017.
https://www.regjeringen.no/no/dokumenter/stprp-nr-95-2008-2009-/id574053/sec9

———. «St.prp. nr. 34 (1999-2000) Om samtykke til godkjenning av EØS-komiteens beslutning nr. 83/1999 av 25. juni 1999 om endring av EØS-avtalens protokoll 37 og vedlegg XI (telekommunikasjonstjenester)», 1999.
https://www.regjeringen.no/no/dokumenter/stprp-nr-34-1999-2000-/id202895/sec1

Forelesningsmateriale

Schartum, Dag Wiese. «Lovgivning: fra utredning til kunngjort lov». Forelesningsmateriale, Universitetet i Oslo, Høstsemester 2011.
http://www.uio.no/studier/emner/jus/afin/DRI2020/h11/Lovgivning%20Fra%20utredning%20til%20kunngjort%20lov.ppt

Tranvik, Tommy. «Dokumentstudier, innholdsanalyse og narrativ analyse.» Forelesningsmateriale, Universitetet i Oslo, Vårsemester 2009.
http://www.uio.no/studier/emner/jus/afin/FINF4002/v09/undervisningsmateriale/metodeforelesning3_tranvik.pdf

Høringer

Arbeids- og administrasjonsdepartementet, Solgunn Tverfjell, og Anne Kristine Hage. Høring - NOU 2003: 21 Kriminalitetsbekjempelse og personvern,
Pub. L. No. 200304521–/AKH, 5 (2004).

Barne- og familiedepartementet, Kristin Berge Vikøren, og Line Berger Husem. Høring: NOU 2003:21 Kriminalitetsbekjempelse og personvern,
Pub. L. No. 200305186/LIBPAS, 2 (2004).

Barneombudet, Knut Haanes, og Anette Storm Thorstensen. Høringssvar: NOU 2003:21 Kriminalitetsbekjempelse og personvern,
Pub. L. No. 03/01200-2, 1 (2004).

Datatilsynet, Georg Apenes, og Hanne Gulbrandsen. HØRINGSUTTALELSE.NOU 2003:21 KRLMINALITETSBEKJEMPELSE OG PERSONVERN,
Pub. L. No. 200372122-2 HPG/-, 11 (2004).

Den Norske Advokatforening, Helge Aarseth, og Merete Smith. Høringssuttalelse - NOU 2003:21 Kriminalitetsbekjempelse og personvern,
Pub. L. No. #16936v1, 3 (2004).

Domstolsadministrasjonen, Sissel Endresen, og Terje Karterud. HØRINGNOU 2003: 21 KRIMINALITETSBEKJEMPELSE OG PERSONVERN,
Pub. L. No. 200301564–4, 2 (2004).

Gudbrandsdal Politidistrikt, og Olav Sørby. Høring - NOU 2003:21 Kriminalitetsbekjempelse og personvern,
Pub. L. No. 2003/01288-3 40, 2 (2004).

Helgeland politidistrikt, og Håvard Fjærli. Høring - NOU 2003:21 Kriminalitetsbekjempelse og personvern,
Pub. L. No. 1082/03, 2 (2004).

Helsetilsynet, Jostein Vist, og Heidi Kristensen. NOU 2003: 21 Kriminalitetsbekjempelse og personvern,
Pub. L. No. 04/288 I HCK, 5 (2005).

Hordaland Politidistrikt, Vidar Refvik, og Svein Erik Krogvold. Høring - NOU 2003:21 Kriminalitetsbekjempelse og personvern - Politiets og påtalemyndighetens behandling av opplysninger,
Pub. L. No. 2003/03273-3 008, 2 (2004).

Juss-Buss, Guro Siljan, og Kjersti Lehmann. Høringssuttalelse - NOU 2003:21 Kriminalitetsbekjempelse og personvern,
Pub. L. No. 719/GS, 3 (2004).

Kommunal- og regionaldepartementet, Hanne Finstad, og Odd Grønvold. NOU 2003:21 - Kriminalitetsbekjempelse og personvern - Høring,
Pub. L. No. 03/4059-4 OGR, 3 (2004).

Kriminalpolitisentralen (KRIPOS), Siri S Frigaard, og Sverre J Wiese Bromander. Høringsuttalelse - NOU 2003:21 - Kriminalitetsbekjempelse og personvern - politiets og påtalemyndighetes behandling av opplysninger,
Pub. L. No. 03/718 008 SJWB, 8 (2004).

Luftfartstilsynet, Sigmund Sandall, og Per Arne Skogstad. NOU 2003:21 Kriminalitetsbekjempelse og personvern,
Pub. L. No. 200304199–4/008/AKA, 2 (2004).

Nasjonal Sikkerhetsmyndighet, og Jan Erik Larsen. Horing - NOU 2003: 21 Kriminalitetsbekjempelse og personvern,
Pub. L. No. 2003/01250-002/NSM/Si/008, 3 (2004).

Nærings- og handelsdepartementet, Kari Bjørke, og Margrethe Norum R. NOU 2003:21 Kriminalitetsbekjempelse og personvern - Høringsuttalelse,
Pub. L. No. 200306445–6/MIR, 2 (2004).

Oslo Politidistrikt, og Hans Halvorsen. Høring - NOU 2003:21 - Politiregisterutvalget,
Pub. L. No. 03/1713, 5 (2004).

Politiets Data- og Materiellltjeneste (PDMT), og Lars Bøhler. Kriminalitetsbekjempelse og personvern - Høring,
Pub. L. No. 2004/00033-3 008, 2 (2004).

Politiets Sikkerhetstjeneste (PST), Arnstein Øverkil, og J.Martin Welhaven. Høringsuttalelse - NOU 2003:21 Kriminalitetsbekjempelse og personvern,
Pub. L. No. 1354/04n, 7 (2004).

Rogaland politidistrikt, Olav Sønderland, og Bjørn Andersen. NOU 2003:21 - Kriminalitetsbekjempelse og personvern - politiets og påtalemyndighetes behandling av opplysninger - Høring,
Pub. L. No. 2003/03146-3 008, 1 (2004).

Romerike politidistrikt, og Hanne Plathe Maartmann. Høring - NOU 2003:21 - Kriminalitetsbekjempelse og personvern - politiets og påtalemyndighetes behandling av opplysninger,
Pub. L. No. 2003/02813-4 411, 2 (2003).

Skattedirektoratet, Lars Nilsen, og Anita Grini. Høring - NOU 2003:21 - Om Kriminalitetsbekjempelse og personvern,
Pub. L. No. 2004/00254 008 fp jbh/mbw, 6 (2004).

Sosial- og helsedirektoratet, Hans Petter Aarseth, og Frøydis Heyerdahl. Høring — NOU 2003:21 Kriminalitetsbekjempelse og personvern,
Pub. L. No. 04/51 74, 3 (2004).

Troms Politidistrikt, Arvid Isaksen, og Ole Bredrup Sæverud. Høring - NOU 2003:21 Kriminalitetsbekjempelse og personvern,
Pub. L. No. 2003/03772-340, 1 (2004).

Utdannings- og forskningsdepartementet, Nille Lauvås, og Per Israelsson. NOU 2003: 21 Kriminalitetsbekjempelse og personvern - horing,
Pub. L. No. 200309106–/PI, 2 (2004).

ØKOKRIM, og Einar Høgetveit. Høring - NOU 2003: 21 Kriminalitetsbekjempelse og personvern,
Pub. L. No. 110/2003, 2 (2004).

Østfold politidistrikt, Ottar Lien, og Hilde Arnesen. Høring - NOU 2003:21 - Kriminalitetsbekjempelse og personvern,
Pub. L. No. 2003/01757-3 008, 7 (2004).

Artikler

Bernt, Jan Fridthjof. «Lovgivning». *Store norske leksikon*, 23. november 2014.
http://snl.no/lovgivning

Datatilsynet. «Internkontroll». Datatilsynet, 13. januar 2012. https://www.datatilsynet.no/regelverk-og-skjema/behandle-personopplysninger/etablering-internkontroll/

Difi. «Internkontroll i praksis - informasjonssikkerhet». Åpnet 19. januar 2018. http://internkontroll.infosikkerhet.difi.no/

Direktoratet for forvaltning og IKT. «Interoperabilitet - overordnet arkitekturprinsipp». Difi.no, 18. august 2017. https://www.difi.no/fagomrader-og-tjenester/digitalisering-og-samordning/nasjonal-arkitektur/prinsipper/interoperabilitet-overordnet-arkitekturprinsipp

———. «PKI (Public Key Infrastructure)», 28. mars 2017. https://www.difi.no/fagomrader-og-tjenester/digitalisering-og-samordning/standarder/standarder/pki-public-key-infrastructure-kravspesifikasjon

Europaportalen. «Hva er Rådet for den europeiske union?» Redaksjonellartikkel. Regjeringen.no, 25. november 2014. https://www.regjeringen.no/no/tema/europapolitikk/fakta-115259/hva-er-radet-for-den-europeiske-union/id734722/

Hansen, Tore. «Norges offentlige utredninger (NOU)». *Store norske leksikon*, 15. februar 2017. http://snl.no/Norges_offentlige_utredninger_(NOU)

Hert, Paul de, og Vagelis Papakonstantinou. «The New Police and Criminal Justice Data Protection Directive: A First Analysis». *New Journal of European Criminal Law* 7, nr. 1 (2016): 7–19. https://doi.org/10.1177/203228441600700102

Hoel Lie, Markus. «mandat – avtale». *Store norske leksikon*, 9. mai 2017. http://snl.no/mandat_-_avtale

Politidirektoratet. «Analyse av politiarbeid på stedet». Politidirektoratet, 29. oktober 2015. https://www.politi.no/globalassets/dokumenter/01-rapporter-statistikk-og-analyse/politiarbeid-pa-stedet/politiarbeid-pa-stedet.pdf

Politiet. «Innsyn i politiets registre». Politiet. Åpnet 6. september 2017. https://www.politiet.no/om/innsyn-og-postjournal/innsyn-politiets-registre/

Regjeringa.no. «Kva er ei høyring?» Redaksjonellartikkel. Regjeringa.no, 29. oktober 2015. https://www.regjeringen.no/nn/dokument/hoyringar/kva-er-ei-hoyring/id2459635/

Skarpenes, Nina. «Politiarbeid på stedet vil løfte politiet». Blogg. www.phs.no, 13. november 2015. https://www.phs.no/om-phs/sjefsbloggen/politiarbeid-pa-stedet-vil-lofte-politiet/

Skulstad, Håkon. «Hvordan forebygge mer og bedre?» *Lensmannsbladet - Politilederen*, Årgang 114, nr. 6 (2011). https://www.politilederen.no/dokumenter/Politilederen/Lensm.bladet%20nr.%206-2011-32s.pdf

Stortinget. «Lovarbeidet». Artikkel. Stortinget, 6. februar 2008. https://www.stortinget.no/no/Stortinget-og-demokratiet/Arbeidet/Lovarbeidet/