

Utdaterte verktøy

En studie av risikoer knyttet til politiets straffesakssystemer

Frøydis Fremstad Wold



Masteroppgave i kriminologi
Institutt for kriminologi og rettssosiologi
Det juridiske fakultet

UNIVERSITETET I OSLO

Vår 2014

Utdaterte verktøy

En studie av risikoer knyttet til politiets straffesakssystemer

Frøydis Fremstad Wold



Masteroppgave i kriminologi

Institutt for kriminologi og rettssosiologi

Det juridiske fakultet

UNIVERSITETET I OSLO

Vår 2014

© Frøydis Fremstad Wold

2014

Udaterte verktøy. En studie av risikoer knyttet til politiets straffesakssystemer.

Frøydis Fremstad Wold

<http://www.duo.uio.no/>

Trykk: Nilz og Otto Grafisk AS

Sammendrag

Utdaterte verktøy. En studie av risikoer knyttet til politiets straffesakssystemer.

Av: Frøydis Fremstad Wold

Veileder: Liv Finstad

Levert ved: Institutt for kriminologi og rettssosiologi, Universitetet i Oslo
Vår 2014

Denne studien tar for seg risikoer¹ knyttet til politiets straffesakssystemer, risikoenes mulige konsekvenser for politiets oppgaveløsning og hva risikosituasjonen gjør med publikum og deres tillit til politiet. Straffesakssystemene er verktøy som skal bidra til at politiet kan løse sine oppgaver på en effektiv måte. For å identifisere viktige utfordringer knyttet til straffesakssystemene har jeg intervjuet informanter med ulike roller innenfor disse systemene. En bruker, en systemspesialist, en straffesaksekspert og en jurist. Diskusjonen i oppgaven konsentrerer seg rundt følgende forskningsspørsmål:

- Politiet er i ferd med å utvikle nye straffesakssystemer. Hvilke risikoer knyttet til dagens straffesakssystemer gjør at det er behov for nye systemer?
- Hvordan påvirker risikoene i straffesakssystemene politiets mulighet for effektiv oppgaveløsning?
- Flere forskere hevder at vi lever i et risikosamfunn. Hva gjør risikoene i straffesakssystemene med de registrerte og publikums tillit til politiet?
- Hvordan snu IKT-utviklingstrenden i politiet for å unngå å komme i en tilsvarende situasjon med utdaterte straffesakssystemer igjen?

Informantene har fortalt at behovet for nye straffesakssystemer er tilstede og at det foreligger flere risikoer knyttet til dagens løsninger. Utfordringene ved straffesakssystemene er kjent både internt og eksternt. Hovedformålet med oppgaven er å bidra til en dypere forståelse av politiets IKT-situasjon sett i et risikoperspektiv og å vise hva som kan skje dersom risikoene blir reelle. Dette drøftes i sammenheng med rettssikkerhet og tillit.

Flere offentlige rapporter har over tid påpekt utfordringer knyttet til straffesakssystemene og politikerne har omsider bevilget penger. Politiet er derfor nå i ferd med å utvikle nye systemer

¹ Ifølge Språkrådet er ordet risiko opprinnelig Italiensk. På norsk bøyes ordet slik: en risiko – risikoen – flere risikoer – alle risikoene.

og MERVERDIprogrammet har ansvaret for utviklingen som forventes ferdigstilt i år 2021. Enn så lenge må politiet leve med utfordringene. Det empiriske materialet mitt viser at det foreligger risiko knyttet til tekniske feil, kodeverk, statistikk, ulik registreringspraksis, kunnskapsdeling og informasjonsflyt. I dette ligger det at det kan oppstå feil i systemene, driftsavbrudd og kollaps. Systemenes lave brukervennlighet gjør at informasjonsinnhenting og registrering er mer komplisert enn det burde være. Noe av det som skaper ekstra press på behovet for nye systemløsninger, er at den kommende politiregisterloven stiller krav til blant annet logging og sporing som dagens systemer ikke imøtekommer. Manglende funksjoner for logging og sporing gjør at det er vanskelig å oppdage dersom noen urettmessig bruker systemene. Det er også vedtatt en ny straffelov som ikke kan tre i kraft fordi det ikke er teknisk mulig for straffesakssystemene å håndtere nytt lovverk. Dagens straffelov er over hundre år gammel, og gjenspeiler derfor ikke, i tilstrekkelig grad, samfunnets oppfatning av rett og galt.

Ifølge informantene, rammer risikoelementene ved straffesakssystemene først og fremst brukerne, ved at de ikke får utført sine arbeidsoppgaver raskt og effektivt, men den praktiske betydningen er vanskelig å måle. Det er ikke slik at risikoene knyttet til systemene er noe politiet velger å ha fordi det gjør at de kan oppklare mer kriminalitet, snarere tvert imot. De registrerte kan også rammes fordi registrert informasjon er mangelfull eller feil. Publikum kan rammes fordi politiet ikke får løst sine oppgaver på en like tilfredsstillende måte som de kunne gjort med nyere straffesakssystemer. Risikoene kunne gjort at publikums tillit til politiet svekkes, men undersøkelser viser at politiet har en relativt høy tillitsrate.

Risikovurderinger er svært utbredt i dagens samfunn. Når det gjelder straffesakssystemene har politiet ikke foretatt systematiske risikovurderinger av dem. Underveis drøftes betydningen av dette, og hva slike risikovurderinger kunne bidratt med. Jeg har identifisert risikofaktorer gjennom mine informanter og sett på noen mulige konsekvenser. Flere kriminologer hevder at mer kunnskap om risiko bidrar til å avdekke mer risiko. Det er et kjent faktum at det er risikoer knyttet til straffesakssystemene, nå er det viktigste å unngå å havne i samme situasjon igjen. Derfor har jeg sett på hvilke tiltak som er satt i gang og foreslår ytterligere tiltak som kan settes i gang for å redusere risikoene.

Abstract

Means out of date. A study on risks in the Norwegian police criminal offences system.

By: Frøydis Fremstad Wold
Supervisor: Liv Finstad
Submitted at: The Department of Criminology and Sociology of Law
University of Oslo
Spring 2014

This paper examines risks in the police computer systems for criminal offences, how the risks affects police work and how the risk situation influence the public and their trust in police. The criminal offence system is a tool that shall make it possible for the police to solve their tasks in an efficient way. To identify important challenges I have interviewed people with various roles within the criminal offence system. One who uses the systems in everyday work, a systems specialist, an expert in criminal justice and one lawyer. The discussion of this paper focuses around the following research questions:

- The police is about to develop new systems for criminal offences. What kind of risks is there in the system of today that makes it necessary to develop new ones?
- How does the risks in the criminal offence systems affect the possibilities for the police to work efficiently?
- Several scientist claims that we live in a risk society. How does the risks in the criminal offences systems affects the registered people and the public trust in police?
- How can the police turn around the non-working technology development trend to avoid getting caught in the same situation again?

The informants explained that there is a need for new criminal offence systems and that there are risks in the systems of today. The current challenge in the criminal offence systems is known by both the police and the citizens. The purpose with this paper is to make people understand the police technology situation in a risk perspective and to show what might happen if the risks becomes real. This will be argued in coherence of rule of law and trust.

Several public reports have over time pointed out the challenges and the politics has at last granted money. Therefore, the police are now developing new systems and a project named MERVERDIprogrammet is responsible for the process, which is expected to be done in the year of 2021. While waiting the police have to live with the challenges. My empiric work shows that there is risks in/for technical errors, codes, statistic, routine nonconformity, knowledge sharing and information flow. That means operation cut, defect and fault is possible. The low user friendliness of the systems makes registration more complicated than necessary. Upcoming new law for registration have requirement for tracking and logging, functionality that is not available today. Lacking functionality for tracking and logging makes it hard to uncover illegitimated use of the systems and makes the pressure for new systems even more highlighted. Also, a new law of penalty is adopted, but it is not valid because the criminal offence systems cannot handle it technically. Today's law of penalty is over 100 years old and therefore the society's view of right and wrong is not reflected in laws currently in force.

According to my informants, the risks in the criminal offence systems first effects the users because they cannot do their job efficiently, but the real effects are hard to measure. The police does not choose to live with the risks in the criminal offence systems so that they can stop more criminals it is rather the opposite.

The registered people can be affected because registered information is uncompleted or wrong. The public might be affected because the police is not able to solve their tasks as satisfying as they could with newer systems. One consequence of the risks might be low trust in the police by the public, but research shows that the police have a high amount of trust.

Analysis of risk is very popular in today's society. The police has not analysed the risks in the criminal offence systems. I discuss the meaning of this and what these analysis could have contributed. I have identified some risks threw my informants and looked at possible consequences. Several criminologists assert more knowledge about risk only contributes to find even more risk. It is a known fact that there are risks in the criminal offence systems, now it is important not to develop the same situation all over again. Therefore I have been looking into what measures that have been done and suggests additional measures that could be made to reduce the risks.

Takk

Å skrive en masteroppgave er en lang prosess som er spennende, utfordrende, frustrerende og meget lærerik. Det er mange som fortjener en stor takk for å ha bidratt til at denne oppgaven har blitt til. Først og fremst vil jeg takke informantene som stilte til intervju og delte sin kunnskap. En stor takk til alle sammen, det er dere som *er* oppgaven! Takk for at dere tok meg godt imot og var hjelpelige med å svare på mine spørsmål.

Jeg vil også gi veilederen min, Liv Finstad, en stor takk. Du har så mye kunnskap som du har delt og tilbakemeldingene fra deg har vært av stor betydning. Ingen kan gi mer motiverende og oppmuntrende ord enn deg. Tusen takk for hjelpen, for din raushet og for at du har lagt til rette for meg.

Så vil jeg takke mastergruppa, Ine, Tanita, Karin og Juni, for gode faglige diskusjoner, konstruktive tilbakemeldinger og hyggelig sosialt samvær. Hvert møte med dere ga masse inspirasjon.

Tusen takk til Camilla, Åse Elise, Eirin og Ingrid, for at dere tok dere tid, stilte opp under korte tidsfrister og bidro med korrekturlesing. Det setter jeg stor pris på!

Takk til Kripos, spesielt mine ledere Heidi og Rune, som har vært fleksible når det gjelder arbeidstid og studiedager.

Denne oppgaven har blitt til på normert tid, ved siden av fulltids jobb, en graviditet og det første leveåret til en liten gutt. Det er jeg utrolig stolt av, men jeg hadde aldri klart det uten hjelp og støtte fra fantastiske venner og familie. Tusen, tusen takk til dere alle. En spesiell takk til alle som har vært barnevakt. All hjelpen betyr så mye for meg! Tusen takk til verdens beste mann, Tom Erik! For din tålmodighet, for ansvaret du har tatt, for alt du har gjort for oss som familie og for at du er stolt av meg. Sist, men ikke minst vil jeg gi en stor takk til Sondre som inspirerer meg hver eneste dag.

Frøydis Fremstad Wold

Nesodden, mai 2014

Innholdsfortegnelse

Utdaterte verktøy	3
Sammendrag	5
Abstract	7
Takk	9
Innholdsfortegnelse	10
1. Introduksjon	13
1.1 Bakgrunn for valg av tema.....	13
1.2 Forskningsspørsmål og tese	15
1.3 Nøkkelbegreper og straffesakssystemene	15
1.4 Oppgavens oppbygging	19
2. Rammeverket	21
2.1 Risikoteori og risikosamfunnet.....	21
2.2 Rettssikkerhet.....	23
2.3 Tillit	25
2.4 Tidligere forskning	26
2.5 Andre teorier	27
3. Veien til målet	29
3.1 Å forske på eget felt	29
3.2 Egen posisjonering.....	31
3.3 Forforståelse.....	33
3.4 Forskningskrav	33
3.5 Fra intervju til analyse	34
3.6 Forskningsresultatenes overførbarhet	39
3.7 Å skrive om et tema i forandring.....	40
4. Straffesakssystemene.....	41
4.1 Risikovurderinger	41
	10

4.2 Driftsavbrudd og kollaps.....	44
4.3 Kodeverk, ulik registreringspraksis og statistikk	47
4.4 Ny straffelov	49
4.5 Effektiv oppgaveløsning?.....	51
4.6 Kunnskapsdeling.....	61
4.7 Snokekultur.....	64
4.8 Situasjonen gir ingen fordeler for politiet	66
5. Risikoenes betydning for publikum og publikums tillit til politiet.....	68
5.1 Rettssikkerhet.....	68
5.2 Datasystemer, kontroll og tillit	70
5.3 Å skape tillit	72
5.4 Publikums tillit til politiet	74
6. Årsaksforklaringer og mulige tiltak.....	79
6.1 Politiets organisering.....	80
6.2 Organisasjonsutvikling, akseptabel risiko og institusjonalisering av avvik.....	83
6.3 Ledelse og risikostyring	86
6.4 Maktanvendelse gjennom datasystemer	88
6.5 Kultur som forklaring.....	91
6.6 Fra isolerte til standardiserte arbeidsprosesser gjennom strategiske virkemidler	93
6.7 Merverdi for fremtidens politi.....	99
6.8 Lærdom fra andre etater og andre land.....	101
7. Avslutning.....	103
Referanser	109
Vedlegg.....	117

1. Introduksjon

1.1 Bakgrunn for valg av tema

Temaet for denne oppgaven er risikoer knyttet til politiets straffesakssystemer BL, Strasak, SSP og BOT², og hvilke mulige betydninger disse risikoene kan ha for politiet, de registrerte, publikum og forholdet mellom dem. Jeg tror det er en alminnelig oppfatning at flere av IKT-systemene til politiet er i dårlig forfatning, og at det er behov for fornyelse. Politiets datasystemer har fått en del oppmerksomhet i media de siste årene. Tungtveiende rapporter som Politianalysen, Rapport fra 22. juli-kommisjonen og Riksrevisjonens undersøkelse av ikt-forvaltningen i straffesakskjeden gir sterk kritikk mot deler av politiets IKT-systemer. Systemene fungerer ikke tilfredsstillende, og de imøtekommer ikke politiets behov. Det er stadig driftsforstyrrelser som rammer produksjon og beredskap (Rapport fra 22. juli-kommisjonen: 333). Rapportene som sier noe om dagens IKT-situasjon er mange, og i løpet av arbeidet med denne oppgaven er det satt i gang flere tiltak for å bedre situasjonen. Både rapportene og tiltakene kommer jeg tilbake til underveis i avhandlingen.

Dagens straffelov er over 100 år gammel. Det betyr at straffebestemmelsene ikke står i forhold til dagens kriminalitetsbilde. Bestemmelsene imøtekommer heller ikke det dagens samfunn ser på som handlinger av strafferettslig karakter. I 2005 ble det, for første gang siden 1902, vedtatt en ny straffelov. Det er ni år siden, men den har enda ikke trådt i kraft, fordi det ikke er teknisk mulig for BL og SSP å håndtere den nye loven. 01.07.14 skal politiregisterloven tre i kraft. Den stiller blant annet krav til sporing og logging, som dagens løsninger ikke imøtekommer. Politietaten er godt kjent med utfordringene og kritikken. Helt siden begynnelsen av 2000-tallet har det vært behov for å lage nye straffesakssystemer. Dagens systemer er mer eller mindre rundt 30 år gamle. Det er på steinaldernivå i den teknologiske verden. Nye systemer er enda ikke på plass, men de er under utvikling. Siste offisielle dato for når utviklingsprosessen skal være ferdig er i år 2021. Da får etaten systemer som har vært etterlengt i nesten 20 år.

Det er flere grunner til at jeg har valgt å skrive om dette temaet. For det første ønsker jeg å skrive om noe som er relatert til min arbeidshverdag. Som sivilt ansatt i Kripos bruker jeg

² I delkapittel 1.3 gjennomgås de ulike systemene og forkortelsene.

politiets straffesakssystemer daglig, bort sett fra BL, og jeg har god kjennskap til disse. Gjennom jobben min opplever jeg til tider utfordringer ved IKT-situasjonen. For det andre har jeg valgt dette temaet fordi det er både samfunnsmessig og faglig aktuelt. Det er utrolig mye som skjer i politiet om dagen når det gjelder IKT. Selv om det har skjedd store endringer underveis vil temaet alltid være aktuelt, fordi det vil være en fare for å havne i samme situasjon igjen. Spesielt dersom det ikke analyseres hva som er galt. Grunnen til at det er mulig å havne i samme situasjon på ny er at teknologien forandrer seg raskt, samtidig som kriminalitetsbildet, lovverket, samfunnet og omgivelsene i politietaten forandrer seg. Alle som har mobiltelefon og pc vet at det stadig kommer nyere og bedre utgaver. Sånn er det også med datasystemer, og derfor er det fort gjort å sitte med utdaterte systemer. For det tredje har jeg valgt å skrive om politiet fordi jeg er fasinert av etaten og har lyst til å forske på den og jobbe i den. Fasinasjonen av politiet handler om etatens sammensatte roller og omfanget av arbeidsoppgaver. Politiets roller og oppgaver kommer jeg tilbake til i kapittel 1.3, samt utover i oppgaven.

Gjennom oppgaven ønsker jeg å beskrive tilstanden til straffesakssystemene, hvordan situasjonen har blitt sånn og hvordan politiet kan unngå å komme i samme situasjon igjen. Jeg ønsker å bidra til en dypere forståelse og peke på elementer som må forbedres gjennom utvikling av de nye systemene. Ettersom etaten holder på å utvikle nye straffesakssystemer er det foretatt utredninger om utfordringene ved dagens systemer og behov. Disse er imidlertid knyttet til arbeidet med å utvikle nye løsninger og vurderer ikke risikoen ved å bruke dagens systemer i ytterligere åtte år.

Det jeg skriver være relevant for utviklingen og gi lærdom med tanke på hvordan politiet bør håndtere straffesakssystemene sine fremover. Jeg har intervjuet personer som har ulike sentrale roller rundt straffesakssystemene. Intervjusedeene er analysert og problematisert opp mot teoretiske perspektiver om risiko. Formålet med dette har vært å bidra med materiale for en dypere forståelse av politiets situasjon. På den kriminologiske fronten har flere forskere (Douglas og Lianos, 2000 og Feeley og Simon, 1998) hevdet at det har skjedd et skifte fra fokus på rettferdighet og behandling til sikkerhet og kontroll. Jeg ønsker å finne ut om straffesakssystemene ivaretar behovet til kontroll mer enn hensynet til rettferdighet, eller om begge deler ivaretas.

1.2 Forskningsspørsmål og tese

Forskningsspørsmålene har endret seg flere ganger underveis. Det har vært en prosess etter hvert som ulike funn har kommet frem og veien har blitt til mens jeg har gått den. Fra første stund har jeg villet skrive om straffesakssystemene til politiet, men hva som skulle vektlegges, vinklingen og hvilke teoretiske perspektiver jeg ville bruke har variert. Til slutt har hovedproblemstillingen blitt som følger:

- Politiet er i ferd med å utvikle nye straffesakssystemer. Hvilke risikoer knyttet til dagens straffesakssystemer gjør at det er behov for nye systemer?

For å sette dette i en kriminologisk ramme har jeg kommet frem til noen forskningsspørsmål som skal støtte opp under hovedproblemstillingen:

- Hvordan påvirker risikoene i straffesakssystemene politiets mulighet for effektiv oppgaveløsning?
- Flere forskere hevder at vi lever i et risikosamfunn. Hva gjør risikoene i straffesakssystemene med de registrerte og publikums tillit til politiet?
- Hvordan snu IKT-utviklingstrenden i politiet for å unngå å komme i en tilsvarende situasjon med utdaterte straffesakssystemer igjen?

På bakgrunn av forskningsspørsmålene har jeg utarbeidet en tese. Forskningsspørsmålene vil sammen med denne tesen danne grunnlaget for diskusjonen i oppgaven.

- Det foreligger risikoer i dagens straffesakssystemer som gjør at politiet får vanskeliggjort sin arbeidssituasjon. Risikoene kan i tillegg påvirke publikum og svekke deres tillit til politiet.

1.3 Nøkkelbegreper og straffesakssystemene

Definering og presisering av nøkkelbegreper er viktig for å avklare utgangspunktet (Johannessen, Tuft og Kristoffersen, 2010: 60-63). Derfor skal noen av oppgavens sentrale begreper avklares i dette delkapittelet.

Politiet er en offentlig myndighet som har sin rolle og oppgaver hjemlet i lov. I politilovens § 1 andre ledd står det følgende: «Politiet skal gjennom forebyggende, håndhevende og

hjelpende virksomhet være et ledd i samfunnets samlede innsats for å fremme og befeste borgernes rettssikkerhet, trygghet og alminnelige velferd for øvrig.»

Politolovens § 2 gir en ytterligere opprømsing av hva som er politiets oppgaver, og det fremkommer at de er sammensatte. De skal beskytte, opprettholde orden, sikre, verne, forebygge, avdekke, stanse, forfølge, hjelpe, yte tjenester, yte bistand, samarbeide med andre virksomheter, drive sivil rettspleie, med mer. Politiet blir ofte omtalt som generalister fordi de har så mange og ulike oppgaver. På den ene siden skal de utøve makt og kontroll, på den andre siden skal de beskytte og hjelpe. St.meld. nr. 42 (2004-2005) slår fast at politiet skal være generalister, og at det heller skal opprettes særorganer ved behov for ekspertise. Dette er under diskusjon. Enn så lenge er politi- og lensmannsetaten organisert med Politidirektoratet over de 27 politidistriktene og de syv særorganene. Politiets sikkerhetstjeneste ligger rett under Justis- og beredskapsdepartementet. Justis- og beredskapsdepartementet er øverste ansvarlig for hele etaten, og skal legge rammer og mål for virksomheten. Departementet har imidlertid delegert mye til Politidirektoratet som skal sikre den faglige styringen, ledelse og utvikling. Hvert enkelt politidistrikt er ledet av en politimester og har egen administrasjon (Politi.no).

Når jeg skriver *politiet* underveis i avhandlingen sikter jeg til etaten og enhver rolle i denne, det være seg jurister, ingeniører, ufaglærte eller politiutdannede.

Straffesakssystemene skal bidra til at politiet kan løse sine oppgaver på en effektiv måte. Systemene jeg har konsentrert meg om er alle en del av straffesakskjeden. IKT i straffesakskjeden omfatter systemer både i domstolene, politiet og kriminalomsorgen, men jeg har begrenset meg til politiets systemer BL, Strasak, BOT og SSP. Grunnen til at akkurat disse systemene er valgt ut, er at de utfyller hverandre i straffesakskjeden. En annen grunn er at jeg mener det er viktige, sentrale systemer som får ufortjent lite oppmerksomhet. Andre systemer som for eksempel PO, Indicia, ATK, Agent og PAL er ikke en del av oppgaven. Det kan finnes straffesaksinformasjon i disse, eller i andre systemer som jeg ikke omtaler, men det blir for omfattende å inkludere systemer som er ment for andre formål enn kun straffesaksinformasjon. For eksempel er PO en operativ logg, Indicia er et etterretningssystem og PAL er en løsning for å ta ut statistikk av andre systemer. Så selv om det kan være straffesaksinformasjon i andre systemer har de andre formål og faller utenfor min

avgrensning. Systemene oppgaven konsentrerer seg rundt er registre som brukes i arbeidet med kriminalitetsbekjempelse. SSP og BOT omtales som reaksjonsregistre, mens BL og Strasak er saksbehandlingsregistre (Kriminalitetsbekjempelse og personvern).

Basis Løsninger (BL) er et saksbehandlingssystem for straffesaker som brukes av både politi og påtalemyndighet. Fra en sak opprettes til den avsluttes registreres alle sakens bevegelser her, og alle dokumenter ligger i BL i sin fulle størrelse. BL er det nyeste av de fire straffesakssystemene. Det ble tatt i bruk første gang i 1996 (Kriminalitetsbekjempelse og personvern). BL har lokale løsninger for de ulike politidistriktene, og systemet kommuniserer med noen andre løsninger (KS1 Konseptvalg).

Strasak er et register for alle straffesaker, og inneholder et uttrekk av opplysninger fra BL. Det registreres ikke direkte i Strasak. All informasjon i Strasak registreres i BL og går automatisk over til Strasak. Til forskjell fra BL finnes det ingen fulle dokumenter her. Strasak danner grunnlag for statistikk til Statistisk sentralbyrå (SSB). Hjemmelsgrunnlaget for Strasak ligger i straffeprosessloven § 62. Strasak har vært i bruk siden 1979 (Kriminalitetsbekjempelse og personvern).

BOT er et bøtere register med opplysninger om personer og foretak som er ilagt bøter, erstatninger, inndragninger og saksomkostninger. Også her hentes registrert informasjon fra BL. Hjemmelsgrunnlaget for registeret ligger i strafferegistreringsloven § 3. Systemet leverer statistikk til SSB og danner grunnlag for attester. Underveis i arbeidet med masterprosjektet ble dette systemet faset ut og informasjonen ligger nå i Strasak (Kriminalitetsbekjempelse og personvern).

Det sentrale straffe- og politiopplysningsregister (SSP) er det nasjonale registeret for straffedømte. SSP har en politiopplysningsdel med personinformasjon og en strafferegistreringsdel med ilagte straffereaksjoner. Hjemmelsgrunnlaget for registeret ligger i strafferegistreringsloven §§ 1 og 4. SSP danner grunnlag for statistikk til SSB og uttak av attester. Registeret består av personopplysninger, reaksjoner, gjenopptakelser, benådning, forvaring, personundersøkelse, rettspsykiatriske undersøkelser, straffegjennomføring, pågripelse, løslatelse, varetekt, signalement, opptaksår for foto, fingeravtrykk og DNA og etterlysninger. SSP ble satt i drift i 1982, systemet er altså 32 år gammelt (Kriminalitetsbekjempelse og personvern).

RESP er forkortelse for Rådet for elektronisk straffesaksbehandling. Rådet ble besluttet opprettet i 2001 og erstatter det som tidligere het Strasakrådet. RESP er en faggruppe som skal gi råd og samordne innen systemforvaltning på straffesaksområdet. Mandatet omfatter systemutvikling, rutiner i straffesaksbehandlingen og opplæring (Rundskriv nr. G-4/2001).

Politiets data- og materieltjeneste (PDMT) er et nasjonalt kompetanse- og servicesenter som skal utstyre politiet med alt de trenger av IKT, materiell, samband, eiendom, bygg og anlegg for å kunne utføre sine oppgaver. PDMT har også det operative ansvaret innenfor IKT-sikkerhet i etaten. Mange av utviklerne ved PDMT er innleide konsulenter på langtidskontrakter og flere har vært der i lang tid. Som et resultat av politianalysen opphørte PDMT som særorgan i 2013. Ansvaret for IKT ligger nå direkte under Politidirektoratet (Rapport, 2013: 26).

MERVERDIprogrammet er et program for merverdi av kunnskap, ressurser og teknologi. Politidirektoratet eier og styrer programmet som ble opprettet høsten 2012. Målet er å utvikle nye straffesakssystemer som en videreføring av en rekke andre mindre prosjekter som har forsøkt å fremme og analysere behovet for nye straffesakssystemer. Ca. 40 personer arbeider i det som nå er forprosjektet. De er fordelt i en styringsgruppe, et politilederforum og en referansegruppe. Styringsgruppen ledes av politidirektøren og består ellers av representanter i sentral ledelse i POD, riksadvokaten, en politimester, direktør for PDMT og sjefen for Kripis. Politilederforumet ledes av assisterende politidirektør og består ellers av ledere fra ulike politidistrikter og Oslo statsadvokatembete. Referansegruppen ledes av politimesteren i Troms og er ellers sammensatt av diverse representanter fra politietaten, kriminalomsorgen, domstolene, fagforeningene, hovedverneombud, Politihøyskolen og Statistisk sentralbyrå. MERVERDIprogrammet antas å slutføres i 2021 (MERVERDIprogrammet informasjonshefte 2013-2014). PDMT arbeider uavhengig av MERVERDIprogrammet, de utvikler og vedlikeholder dagens systemer frem til det kommer nye.

Når det gjelder kostnadene til programmet ble de i 2012 estimert til ca. 2,4 milliarder kroner (KS1 konseptvalg, 2012: 6).

Politiregisterloven ble vedtatt i 2010 og den er ventet å tre i kraft 01.07.14. Lovens § 1 sier at «Formålet med loven er å bidra til effektiv løsning av politiets og påtalemyndighetens oppgaver, beskyttelse av personvernet og forutberegnelighet for den enkelte ved behandlingen av opplysninger» (politiregisterloven). Videre reguleres lovens virkeområde i § 3:

Loven gjelder for politiets og påtalemyndighetens behandling av opplysninger, med unntak av behandling av opplysninger som

1. reguleres av lov 16. juli 1999 nr. 66 om Schengen informasjonssystem (SIS),
2. er del av politiets forvaltningsvirksomhet eller sivile gjøremål.

Forvaltningsvirksomhet i Politiets sikkerhetstjeneste er likevel omfattet av loven.

Loven gjelder elektronisk behandling av opplysninger, og manuell behandling av opplysninger når disse inngår eller skal inngå i et register.

For opplysninger om gjenstand gjelder kapittel 4 og reglene om taushetsplikt i den grad opplysninger omfattes av § 23.

Loven gjelder også for Svalbard, Jan Mayen og de norske bilandene, med de endringer som Kongen fastsetter av hensyn til de stedlige forhold (politiregisterloven).

1.4 Oppgavens oppbygging

Etter dette introduksjonskapittelet presenteres teoretisk stoff om risiko og tillit i kapittel 2. Det er disse perspektivene som hovedsakelig er brukt i oppgaven og de utgjør den kriminologiske rammen. Rettssikkerhetsbegrepet drøftes også i kapittel 2, i tillegg til at det blir en gjennomgang av andre teoretiske perspektiver som kunne vært benyttet i større grad. Jeg vil også si noe om hvordan andre teorier kunne påvirket perspektivering av forskningsfunnene.

Kapittel 3 er et metodekapittel hvor det redegjøres for hvordan oppgaven har blitt til, metodiske valg og etiske refleksjoner.

I kapittel 4 blir det en gjennomgang av dagens straffesakssituasjon. Her presenteres risikoene informantene vektla i sine intervjuer og det drøftes hva risikoene betyr for politiet og de registrerte.

Det 5. kapittelet handler om rettssikkerhet og tillit. Her går diskusjonen på risikoenes påvirkning av rettssikkerheten. Sammen med rettssikkerhet drøftes publikums tillit til politiet.

Informantene hadde tanker rundt dette som jeg sammenligner med undersøkelser om tillit til politiet.

Kapittel 6 handler om mulige årsaksforklaringer som kan ha bidratt til at politiet nå befinner seg i en situasjon med risikofylte straffesakssystemer. Disse årsaksforklaringene danner også grunnlaget for mulige tiltak som kan igangsettes.

Kapittel 7 er det avsluttende kapittelet som danner en konklusjon for oppgaven.

Til slutt er litteraturlisten oppført og deretter ligger vedleggene. Vedleggene inneholder intervjuguidene som ble brukt under intervjuene, informasjonsskrivet til informantene og godkjenningen av prosjektet fra Norsk samfunnsvitenskapelig datatjeneste (NSD).

2. Rammeverket

2.1 Risikoteori og risikosamfunnet

Risikoteori er teori om hvordan risiko påvirker sosiale forhold og omvendt. Begrepet risiko oppstod ifølge sosiologen Niklas Luhman (1993: 9) sent i middelalderen, eller tidlig i moderne tid. Det var også brukt tidligere, men i mindre grad og i andre sammenhenger enn i dag. I dag sier begrepet noe om sannsynligheten for tap og graden av det eventuelle tapet. Adam og Van Loon (2000: 7) skriver at risiko opprinnelig handlet om økonomisk forsikring under handel, forholdet mellom lege og pasient og det å risikere noe for å redde andre. Risiko var på den måten noe som knyttet seg til bestemte handlinger.

I flere forskningsmiljøer omtales dagens samfunn som et risikosamfunn. Risikosamfunnet er ikke noe borgerne velger å være en del av eller ikke. Det er strukturelle forhold som skapes gjennom avansert industrialisering. I det moderne samfunn er menneskene opptatt av beskyttelse mot det uønskede, ukjente og farlige. Hudson (2003: 43) forklarer det negative fokuset som ligger i risikosamfunnet med forståelsen av industrialiseringen. Hun mener at folk forbandt noe annet med industrialisering før enn nå. Før tenkte folk på arbeidsplasser, muligheten til å tjene mer penger og høyere levestandard. Altså en positiv assosiasjon. I dag forbindes industrialiseringen mer med forurensing, miljøskader, arbeidsledighet og mindre familietid. Det er det som kan risikeres og det negative som er det sentrale (Hudson, 2003: 44).

Risikosamfunnet er et samfunn med krav til sikkerhet gjennom overvåkning og risikovurderinger. «The essence of risk is not that it is happening, but that it might be happening» (Adam og Van Loon, 2000: 2). Risiko er konstruksjoner hvis det motsatte er å være virkelig nettopp fordi det *kan* skje, det skjer ikke (Adam og Van Loon, 2000: 24). Alle kan konstruere risiko, men det er kun sannsynlig risiko som betyr noe. Scott Lash presenterer en alternativ måte å se risiko på. I stedet for et risikosamfunn mener han det er relevant å snakke om en risikokultur. Et risikosamfunn kan forstås som noe determinerende, institusjonelt, normativt og regelbundet, mens en risikokultur er en mer fleksiv, dynamisk og fleksibel måte å se risiko på. Risikokulturen er ikke like bundet og institusjonell som risikosamfunnet (Lash, 2000: 47). Lash mener det passer bedre i dagens samfunn enn teorien om risikosamfunnet, som er en mer låst form å se risiko på. Det er ikke min intensjon å utdype kontrasten mellom disse risikoperspektivene, men jeg vil påpeke at det er flere

forståelsesmåter innen risikoteori. Min posisjon i dette prosjektet ligger i perspektivet om et risikosamfunn.

Ragnar Hauge skriver om risikosamfunnets kriminologi. Han hevder at kriminologien har fått en ny oppgave, nemlig å beskrive trusselbilder. Tradisjonelt har kriminologien og strafferetten vært opptatt av individet som lovbrøttere og å forklare kriminalitet og avvik. Risikoteori søker vekk i fra individet, og fokuserer på det som statistisk sett anses som farlig og derfor må kontrolleres (Hauge, 2001: 155-156). Risikosamfunnet henger videre sammen med overvåkningssamfunnet. For å kunne kontrollere det farlige må det overvåkes (Hauge, 2001: 157). Overvåkningsaspektet ligger imidlertid utenfor diskusjonen i denne oppgaven. Jeg har valgt å utføre mitt prosjekt gjennom et risikoperspektiv, men *hvem* som er farlige eller hvordan grupper som utgjør en risiko kartlegges, er ikke tema her. Derimot skal jeg se på noen av de verktøyene politiet bruker i sin oppgaveløsning, og hva som kan utgjøre risikoer innenfor disse verktøyene. Jeg skal undersøke hvordan politiet forholder seg til risikoer innad i etaten og hva som kan skje dersom risikoene som foreligger utløses.

Risikovurderinger er en strukturert måte å konstruere et bilde av hva som er usikkert, hva som kan skje dersom risikoen blir reell og hvordan både usikkerheten og det reelle kan håndteres (Ericsson og Haggerthy, 1997, Adam og Van Loon, 2000, Luhman, 1993, Feeley og Simon, 1998). I dagens samfunn gjør vi det vi kan for å unngå det vi opplever som tap (Luhman, 1993: 13). Stadig flere organisasjoner og bedrifter har arbeidsoppgaver som går på å gjennomføre risiko- og sårbarhetsanalyser. Det er også mulig å ta høyere utdanning innen risikoanalyse og risikostyring. Dette viser at samfunnet vårt er opptatt av risikovurderinger. Luhman (1993) skriver at vi mennesker forholder oss til og vurderer risiko hver eneste dag. Sosiale systemer i det moderne samfunn er mer opptatt av risiko enn tidligere. Vi aksepterer ikke lenger hendelser uten å se på sammenhengen mellom en vurdering og et utfall.

Ettersom risikovurderinger er en del av det moderne samfunn er det interessant å se hvordan det gjenspeiler seg i politiets måte å håndtere egne straffesakssystemer. Risiko handler om mulige fremtidige hendelser og følgende konsekvenser. Risiko er det usikkerhetsmomentet som kan knyttes til de eventuelle konsekvensene. I denne oppgaven brukes betegnelsen risiko om kombinasjonen av hendelser i straffesakssystemene, eller hendelser med rot i straffesakssystemene, og konsekvensene av disse hendelsene. Usikkerheten handler om

sannsynlighet, om hendelsen vil inntreffe og hvilke konsekvenser som kan oppstå. Gjennom et kriminologisk risikoteoretisk perspektiv skal jeg si noe om hvordan situasjonen påvirker menneskene rundt systemene. I kapittel 4 og 5 skal jeg vise hvilke risikoer som foreligger i straffesakssystemene, samt diskutere hvordan risikoene påvirker politiets oppgaveløsning, publikum og rettssikkerheten. Sentrale forfattere innen risikoteori som jeg benytter meg av er Luhman (1993), Ericson og Haggerty (1997) og Chan (2003).

Northrop, Kraemer og King (1995) tar for seg datainnføringens påvirkning av politiets effektivitet og har spesielt fokus på opplæring. De skriver: «It was found that the respondents in forty-four cities across the United States view computers as a major force in the fight against crime» (Northrop mfl., 1995: 259). Flere forskere skriver om datasystemenes inntog som en særdeles viktig faktor for kriminalitetsbekjempelse (Chan, 2003, Northrop mfl., 1995 og Ericson og Haggerty, 1997). Nå er nok ikke straffesakssystemene de viktigste systemene norsk politi har for dette formålet, men det er absolutt ett av formålene med systemene. Derfor trekker jeg paralleller fra slike studier til mitt prosjekt i kapittel 4.5.

2.2 Rettssikkerhet

Risikoene som fremlegges i oppgaven kan tenkes å påvirke samfunnets borgere. Hvordan, hvorfor og om det har betydning for rettssikkerheten blir drøftet sammen med risikoene i kapittel 4 og sammen med tillit i kapittel 5, men noen ord om rettssikkerhetsbegrepet kommer allerede her.

De fleste har et forhold til hva som ligger i begrepet rettssikkerhet, men det finnes ulike forståelser og definisjoner. Ifølge Store norske leksikon er rettssikkerhet «sikkerhet trygget gjennom rettsordenen». Jeg synes det som står i Skjult informasjon – åpen kontroll (2009: 60) er mer oppklarende: «Kjernen i begrepet «rettssikkerhet» er knyttet til krav om at enkeltindividet skal være beskyttet mot overgrep og vilkårlighet fra myndighetenes side, samtidig som vedkommende skal ha mulighet til å forutberegne sin rettsstilling og forsvare sine rettslige interesser.» Robberstad har i sin doktorgrad en mer utvidet definisjon. Hun skriver at vi kan snakke om en klassisk betydning og en nyere forståelse av rettssikkerhet. I den klassiske betydningen omfatter begrepet statens ansvar for å beskytte borgerne mot å bli

utsatt for angrep av staten *og av andre borgere* (Robberstad, 1999: 360). Den nyere forståelsen er at staten har et ansvar for å beskytte borgere mot overgrep kun fra staten (Robberstad, 1999: 362-362). Jeg kommer til å bruke ordet i sin klassiske betydning, altså i en videre forstand enn den moderne. Hovedgrunnen til det er at jeg ikke vil innskrenke forståelsen av rettssikkerhetsbegrepet fordi den klassiske versjonen av begrepet gir en mer fullstendig forståelse av de rettssikkerhetshensyn politiet må ivareta.

Staten kan håndheve retten med tvang, og politiet skal bruke makt i nødvendige tilfeller for at borgerne skal etterleve samfunnets normer. Alle, også de som har begått lovbrudd, har krav på rettssikkerhet. Det betyr at alle individer har rett til å beskyttes mot at staten misbruker sin makt, og at alle har rett til å beskyttes mot overgrep fra andre borgere. Det finnes rettssikkerhetsgarantier som kan benyttes i tilfeller hvor et individ føler seg usikker på statens maktanvendelse. Rettssikkerhetsprinsipper er også utviklet for å ivareta fordeling av goder og tjenester fra staten. Man kan ikke avskjæres fra å få fellesgoder som for eksempel sosialstøtte, pensjon og helsehjelp uten grunn (Boe, 1993: 368).

Rettssikkerhet er noe mennesker har vært opptatt av i mange hundre år, men med de senere års teknologiutvikling har det kommet nye problemstillinger. For å sikre rettssikkerheten må IKT-systemer innrettes slik at det ikke oppstår risiko for å fatte beslutninger på feil grunnlag. Ifølge Boe (1993: 375) er faremomentet at registrert informasjon kan bli brukt i andre sammenhenger og til andre formål enn den var ment for. Bernt og Doublet (1999: 350) argumenterer på samme måte som Boe. De mener at rettssikkerhet dreier seg om hvordan forvaltningsvedtak blir truffet og vedtakenes innhold. På samme måte som Robberstad hevder Bernt og Doublet (1999: 353-354) at det har skjedd et skifte i oppfattelsen av rettssikkerhet mot en videre forståelse. Likevel trekker de det ikke like langt som Robberstad. Bernt og Doublet (1999: 353) mener den moderne forståelsen går på velferdsstatens ansvar for å sikre alle de samme godene. De skriver ingenting om å sikre borgerne mot hverandre.

Om risikoen i straffesakssystemene påvirker rettssikkerheten drøftes både i kapittel 4 og 5. Informantenes tanker om rettssikkerhet presenteres i kapittel 5 sammen med tillit.

2.3 Tillit

Barbara Hudson (2003) hevder at i betydningen av risikosamfunnet ligger det underforstått at risiko er en del av den daglige tankegangen, både til enkeltpersoner og til organisasjoner.

Rutinegjørelsen av risikotenkning henger nøye sammen med hvordan vi forholder oss til andre mennesker. Det er ikke gitt at vi har tillit til andre, tillitsmottakeren må vise seg tilliten verdig (Hudson, 2003: 44). Risiko henger altså sammen med tillit, og jeg skal derfor drøfte risikoens betydning for publikums tillit til politiet i kapittel 5.

Grimen (2009) beskriver hva tillit er, og han bruker tillit til staten som et eksempel. Politiet er en statlig aktør, og beskrivelsen er derfor relevant. Tillit er å stole på andre selv om det er fare for tap, ifølge Grimen. Han mener at det er en stadig synkende tillit til politiske institusjoner og profesjoner i Vesten. Folk flytter og reiser mer. Stadig nye relasjoner skaper utfordringer når det gjelder å skape tillit. Nye kommunikasjonsmåter, økonomiske kriser og avhengighet av viktige institusjoner påvirker tilliten mellom folk (Grimen, 2009: 9). Hovedpoenget til Grimen er å vise at tillit er å handle med få forholdsregler. Han skriver at alternativet til hans forklaring er å se tillit som en type oppfatning eller forventning (Grimen, 2009: 134). Grimen mener derimot at forventningene bidrar til hvordan man velger å handle. Tillitsgivere har forventninger til at tillitsmottakeren er pålitelig (Grimen, 2009: 26). Tillit gir også makt ved at noen har noe i andres varetekt (Grimen, 2009: 135). Grimen forklarer hvordan risiko, makt og tillit henger sammen, dette kommer jeg nærmere inn på i kapittel 5.

Ifølge Larsson (2010) henger forståelsen av tillitsbegrepet sammen med samfunnsendringer som har skjedd de siste ti år. Han trekker frem overgangen fra kontanter til virtuelle penger, fremveksten av internett, bedret kommunikasjonsmuligheter, politiske omveltninger, forandringer i produksjonsforhold, globalisering og utdanningsekspløsjonen (Larsson, 2010: 10-12). De nye kommunikasjonsmåtene og den nye måten samfunnet er bygd opp på krever tillit mellom borgere og fra samfunnsborgerne til institusjoner. Betydningen av tillitsbegrepet har utviklet seg parallelt med risikosamfunnet. «Vi forventer at politiet skal være eksperter og hjelpe oss med et bredt spekter av problemer og onder. Når man ser at de ikke alltid lykkes i dette, noe som i seg selv er umulig, vil kritikk ramme politiet», skriver Larsson (2010: 13). Med så stort spenn av arbeidsoppgaver som politiet har er det ikke rart at de stadig er i søkelyset og blir forsket på. Kontrastene i arbeidsoppgavene forutsetter prioritering og det er vanskelig å oppfylle alle krav. Politiet er avhengig av tillit hos befolkningen og må derfor

være flinke til å gi informasjon, oppfylle forventninger og inkludere publikum. Undersøkelser viser at politiet har tillit i befolkningen (St.meld. nr. 42). I kapittel 5 viser jeg til flere undersøkelser om tillit til politiet, og jeg sier noe om hvordan risikoen i straffesakssystemene kan tenkes å påvirke publikum.

2.4 Tidligere forskning

Det finnes ikke mye forskning om mitt tema. Risiko, politi, IKT og tillit er det store mengder litteratur om hver for seg, men de fire temaene i sammenheng er det derimot mindre av.

Flere NOU-er er relevante for oppgaven fordi politiets utfordringer har blitt påpekt i disse. Spesielt har Politianalysen bidratt til at IKT i politiet er et hett tema. Politianalysen er derfor mye brukt i denne oppgaven.

Av mer forskningsbasert norsk litteratur har jeg sett på Helene Oppen Gundhus (2006), Torill Iversen (2012) og Tore Hartvigsen (2013). De har sett på politiets bruk av IKT, men ikke på selve systemene. Hartvigsen er særlig relevant når det gjelder risikoanalyser. Gundhus skriver mye om det å være kunnskapsbasert. Dag Wiese Schartum har skrevet en del om IKT i forvaltningen generelt, med vekt på det juridiske. Jeg bruker Schartum i kapittel 4.6 for å belyse forskjellen mellom menneskefeil og systemfeil og hvorfor intern kontroll er viktig. I kapittel 6.3 og 6.5 bruker jeg Schartum for å vise hvordan makt kan oppstå i systemer og i skjemaer.

Av internasjonal litteratur henviser jeg mye til Ericson og Haggerty (1997) og Janet Chan (2001 og 2003). Deler av deres bidrag treffer kjernen i denne oppgaven da de skriver om risiko, politiets bruk av IKT og politiets oppgaveløsning. Deres bidrag kommer spesielt frem i kapittel 4.5, men også flere steder i kapittel 6.

I kapittel 6 bruker jeg organisasjonssosiologen Diane Vaughan. Hun har relevans for denne avhandlingen gjennom sin forklaring av hvordan organisasjoner systematisk produserer avvik og tøyser grensene for det som anses som akseptabel risiko.

2.5 Andre teorier

Risikoteori er et relevant rammeverk for denne oppgaven. Andre perspektiver jeg kunne anvendt er for eksempel maktteori eller kulturteori. Det ville gitt en annen oppgave, samtidig kan det påpekes at en teori ikke utelukker en annen. Jeg vil til en viss grad bruke også disse perspektivene, selv om de ikke danner rammen for oppgaven.

Skulle jeg brukt maktteori som teoretisk perspektiv ville oppgaven konsentrert seg mer rundt politiet som en del av statsmakta, hva som ligger i denne makta og hvordan den utøves gjennom straffesakssystemene. Jeg måtte diskutert forholdet mellom stat og rett inngående og satt meg inn i ulike definisjoner av makt og perspektiver innen maktteori. Maktteori kunne vært nyttig for å forstå politiet sin rolle i samfunnet. Et av mine funn går på at risikoene som er knyttet til straffesakssystemene ikke gir noen fordeler for politiet. Hadde jeg gått mer inn i et maktperspektiv, måtte jeg diskutert hva risikoene har å si for politiets maktutøvelse. I stedet har jeg lagt vekt på hva risikoene har å si for effektiv oppgaveløsning og hvordan publikum merker risikoene. I et maktperspektiv kunne jeg skrevet mer om den politiske styringen og organiseringen av politiet enn det jeg har gjort i denne oppgaven. I stedet har jeg konsentrert meg om risikofaktorer for å kunne dra lærdom av det.

I oppgaven diskuterer jeg også forholdet mellom lov og samfunn. Det er et interessant spenningsfelt som jeg ville studert nærmere om jeg hadde skrevet en rettssosiologisk oppgave. En studie i den retningen kunne innebære et systemteoretisk perspektiv på virkningene mellom rett, tvang, moral og politikk, mens denne oppgaven er et systemteoretisk perspektiv mellom risiko, rettssikkerhet og tillit.

Kulturen i politiet kan påvirke risikoen i straffesakssystemene, men straffesakssystemene kan også påvirke kulturen i politiet. Dette skriver jeg om i kapittel 4.7.

Ifølge Hayward og Young (2004: 259) er *cultural criminology*³ et perspektiv som ser kriminalitet og kriminalitetskontroll som kulturelle produkter. Fokuset er på regler som brytes

³ Jeg velger å oversette *cultural criminology* direkte til *kultur kriminologi*. Begrepet kan forstås som en retning innen kriminologien hvor både kriminalitet, samfunnskontroll og retten anses som produkter av kulturelle verdier.

og tilblivelsen av regler, med vekt på kreative konstruksjoner. Utvidelsen av rettssystemet med fengsler, politi, behandlingstilbud, forebygging og det akademiske miljøet i den vestlige verden har hatt betydning for fremkomsten av kulturkriminologien (Hayward og Young 2004: 261). Hvis jeg hadde brukt kulturteori som ramme for oppgaven ville hovedforklaringen for hvordan politiet var kommet i en situasjon med utdaterte straffesakssystemer, være kulturbetinget. Med dette mener jeg at det ville vært politiets yrkeskultur som var hovedårsaken til at de sitter med utdaterte verktøy til sin oppgaveløsning. Kulturbegrepet favner mye og jeg drøfter kultur som årsaksforklaring for dagens situasjon i kapittel 6.4, men jeg mener det ville være begrensende for oppgaven å bruke kultur som selve rammeverket for oppgaven.

3. Veien til målet

I dette kapitlet redegjør jeg for metodiske valg og etiske refleksjoner som er gjort underveis i prosjektet. Det er av stor betydning for forskningens kvalitet at jeg som forsker argumenterer for og dokumenterer hvert skritt i prosjektet (Thagaard, 2006). Gjennom hele prosessen har det vært et mål å oppfylle forskningskrav, vitenskapelige kvalitetskriterier og etiske prinsipper så godt som mulig.

3.1 Å forske på eget felt

Asbjørn Rachlew er en politimann med doktorgrad i kriminologi som har forsket på eget felt. Han skriver at det er en balansegang mellom å ha nødvendig analytisk distanse til feltet man forsker på og å ikke bli for teoretisk eller virkelighetsfjern (Rachlew, 2010: 131). Når det presenteres et materiale kan meningen oppfattes ulikt avhengig av hvem som er avsender (Rachlew, 2010: 133). Politiet er trolig mer hårsåre for det som sies av sine egne, enn det som uttrykkes av utenforstående ettersom internt personell har en dybdekunnskap som utenforstående ikke har. Rachlew mener at en innsideforsker vil å ha en fordel av sin egen rolle i planleggingsfasen av et forskningsprosjekt, men på en annen side har innsideforskeren en forestilling som kan gjøre blind for andre synsvinkler enn sin egen (Rachlew, 2010: 135).

Som ansatt på Kripos har jeg fordel av at jeg har et kontaktnettverk som har vært hjelpelige med å skaffe informasjon og informanter. Min bakgrunnskunnskap og erfaring gjør at jeg lettere har et bilde av hvor informasjon kan finnes og hvilke spørsmål som burde stilles under intervjuene for å belyse temaet. Det er også en fordel at jeg ikke har måttet sette meg inn i politiets straffesakssystemer fra bunn, fordi jeg hadde god kjennskap til dem fra før.

Ulempen med å forske på et felt som også er jobben min er at jeg får en slags dobbeltrolle som jeg må være veldig bevisst. Jeg må blant annet sikre at jeg skiller mellom hva som er offisiell informasjon og hva som er intern og/eller konfidensiell informasjon. Å være klar over hvilke kilder jeg bruker til enhver tid har vært helt sentralt for å unngå at jeg bruker taushetsbelagt informasjon. Dette har jeg vært svært bevisst på gjennom hele prosessen. I store deler av tiden hvor masteroppgaven er skrevet har jeg vært i mammapermisjon. Av den grunn har jeg sluppet å veksle mellom rollen som arbeidstaker og forsker i det daglige. De

periodene jeg måtte veksle mellom rollene synes jeg det fungerte greit fordi jeg brukte mye tid på å reflektere over hvor jeg fikk informasjon fra og hvordan.

Alver og Øyen (1997: 69) mener det er viktig å avklare forskerens ståsted og utgangspunkt. Jeg må huske på at jeg kan være preget av min egen kunnskap og erfaring. Jeg ser ikke temaet med forutsetningsløse øyne. Dette kan både være en fordel og en ulempe. Underveis i prosjektet har jeg tenkt gjennom og reflektert over hvordan jeg kanskje ville sett ting med andre øyne. For eksempel har jeg tenkt mye på mitt utgangspunkt som bygger på min arbeidserfaring og hvordan utgangspunktet ville vært dersom jeg aldri hadde jobbet på Kripos. Andre har et inntrykk av politiet basert på sine erfaringer. Enten gjennom media eller basert på et møte med politiet. Jeg kan bare forestille meg hvordan andre ville oppfattet det samme som meg, men dette er likevel forestillinger som danner grunnlag for noen refleksjoner som igjen gjør at jeg kanskje møter mine funn på en åpen måte. På denne måten håper jeg at jeg ikke har latt meg styre eller bli villedet av min bakgrunn.

For å få gode intervjuer er det viktig å skape et tillitsforhold. Jeg tror at utgangspunktet mitt som arbeidstaker i politiet gjorde at jeg hadde et godt utgangspunkt for å skape tillit. Kanskje for mye tillit ved at informantene kunne ville dele mer enn de burde i form av sin stilling. Det er viktig for meg å kunne forsvare oppgaven både ovenfor forskningen og ovenfor arbeidsplassen min. Mitt ønske er utelukkende å bidra til forbedring. Jeg har stor tiltro til politiet og rettssystemet i Norge selv om jeg mener det er relevant å drøfte begreper som rettssikkerhet og tillit. Det er en samfunnsinteresse å oppnå forbedringer og for å gjøre det må utfordringene som foreligger diskuteres. Kripos ytret at de "helst ikke" ville at jeg hadde informanter ved Kripos fordi kolleger lett kunne glemme at jeg er student og ikke medarbeider og dermed gi meg taushetsbelagt informasjon. Det skapte utfordringer for meg fordi jeg hadde behov for noe av den kunnskapen som kun ansatte ved Kripos har. Derfor intervjuet jeg likevel én person fra Kripos. For å sikre bevissthet rundt min rolle som student ga jeg informantene et informasjonsskriv på forhånd hvor det ble presisert at dette er et studentprosjekt. Informasjonsskrivet er vedlagt denne oppgaven (vedlegg 5). Ved intervjustart ble min rolle påpekt på nytt.

Det kan være utfordrende å skrive om egen arbeidsplass. For å sikre best mulig tillit har jeg hatt dialog med arbeidsgiver om hva som har vært mine mål og hvordan jeg har gått fram for å nå målene. Prosjektbeskrivelsen, informasjonsskriv og intervjuguider er lagt frem for

arbeidsgiver i forkant av prosjektet og Kripos hadde, etter en gjennomgang av dette, ingen merknader til arbeidet med oppgaven.

Jeg har også forberedt meg på at media kan rette oppmerksomhet mot oppgaven fordi jeg som innsideforsker kritiserer noen sider ved politiet.

Media har en spesiell, kontrollerende rolle ovenfor politiet. Funn som indikerer normative avvik i politiets virksomhet, blir raskt nyhetsstoff, og kommer kritikken fra innsiden vet jeg av erfaring at kombinasjonen risikerer å skape store overskrifter. Ikke nødvendigvis fordi forskningen, isolert sett fortjener så stor plass, men fordi kritikk fra innsiden, fortsatt er så uvanlig at det gir assosiasjoner til sensasjon og skandaler (Rachlew, 2010: 147).

Jeg har det fulle og hele ansvaret for det som presenteres i oppgaven selv om det bygger på intervjuene av informantene.

3.2 Egen posisjonering

Som beskrevet har jeg en dobbeltrolle ved å være ansatt i politiet og forske på eget felt. Jeg har forsøkt å posisjonere meg og vil nå gjøre rede for min rolle som forsker. Cecilie Høigård (2005: 105) skriver at det er en kløft mellom to politiforskningsmiljøer; universitetsforskningen og myndighetsforskningen. Myndighetsforskning er forskning *for* politiet. Høigård skriver at myndighetsforskningen er preget av et styrings- og ovenfraperspektiv. Forskningen inneholder lite teori og er bundet av organisasjonens verdier. Myndighetsforskningen har til formål å være nyttig og veiledende for politiets arbeidsmåter og prioriteringer. Hadde Kripos vært min oppdragsgiver for denne oppgaven ville jeg befunnet meg i dette forskerlandskapet, men det gjør jeg ikke fordi formålet med oppgaven er ikke å utføre en studie *for* politiet. Selv om jeg jobber for Kripos og skriver om et tema som er relatert til min arbeidshverdag, så er det ikke dette Høigård kaller myndighetsforskning. Den andre rollen Høigård skriver om er forskning *om* politiet, som er den klassiske universitetsforskningen. Universitetsforskningen inneholder mer teori, er mer kritisk og friere enn myndighetsforskningen. Rachlew (2010: 145) foreslår innsideforskeren som en løsning på Høigård (2005: 107) sin etterlysning av en bro mellom de to forskerposisjoneringene fordi innsideforskeren har en fot innenfor begge forskningslandskapene. Innsideforskeren er altså en som forsker på sine egne.

Da jeg begynte på master i kriminologi spurte jeg Kripas om de ønsket at jeg skulle studere et tema som kunne være aktuelt for Kripas. Det takket de nei til. Hadde de bedt meg om å skrive om et spesifikt tema ville denne oppgaven blitt en sammensetning av de to rollene Høigård (2005) presenterer. Det kunne bydd på noen utfordringer fordi forskningen ville blitt virksomhetsstyrt. Av de overnevnte rollene er altså min posisjonering forskning *om* politiet. Likevel preges jeg nok av min bakgrunn som ansatt i politiet, og det vil sannsynligvis virke inn på det jeg skriver i form av hva jeg velger å vektlegge. Valget av temaet er også et resultat av at jeg er preget av min bakgrunn. Straffesakssystemene til politier er noe som engasjerer meg. En av de første tilbakemeldingene jeg fikk fra universitetet på oppgaven, var at den var preget av å ligne en virksomhetsrapport. Da tok jeg noen grep, endret forskningsspørsmålene og fokuserte mer på teori. Jeg ønsker å unngå å skrive en virksomhetsrapport *for* politiet, samtidig er min ambisjon at det jeg skriver appellerer *til* politiet og at de anser den som relevant. Formålet er altså å skrive en oppgave *for* universitetet, *om* politiet, *til* begge. Dermed er jeg kanskje et eksempel på en innsiddeforsker som Rachlew (2010) mener bygger en bro mellom myndighetsforskningen og universitetsforskningen.

Waddington bringer på banen det han kaller *Critical friend* som jeg velger å oversette direkte til *kritisk venn*. Waddington (2010: 119) skriver at politiet har mange kritiske venner hvor akademiske forskere er en av dem. Kritiske venner kan presentere et tema for publikum med en frihet som politiet ikke har selv. De kan også bruke en type ekspertise som politiet ikke nødvendigvis har tilgang til. En kritisk venn er gjerne en som bruker mye tid på politiet, viser forståelse for politiets situasjon og skriver på en måte som viser seg tillit verdig. Samtidig er perspektivet kritisk og kommer kanskje med modige forslag. I tillegg er den kritiske venn en som er uavhengig, altså en som ikke jobber i politiet. Jeg vil tro at Liv Finstad er et godt eksempel på denne posisjoneringen.

Waddington skriver om politiets bruk av biljakter som metode for å stoppe lovbrøttere. Mange biljakter ender med dødsfall. Poenget til Waddington er at døden kunne vært unngått hadde politiet brukt andre metoder enn å forfølge noen med bil i høy hastighet. Waddington ser seg selv som en kritisk venn. I det ærend foreslår han å endre metodene for å stanse de som vanligvis forfølges i biljakter. Som han skriver, kommer han med provoserende forslag for å endre en diskusjon og skape debatt. Dette gjør han for å vise hva kritisk akademisk vennskap

kan bety i praksis og for politiet (2010: 125). Jeg ønsker å være en kritisk venn, men kan ikke plassere meg i denne posisjonen, da det at jeg er ansatt i politiet setter visse føringer for valg av tema i oppgaven. Ingen av mine funn er sensurert for denne oppgaven, men hadde noen av funnene gått over min publiseringsgrense ville jeg kanskje funnet et annet tema. Jeg mangler derfor den friheten og uavhengigheten som Waddington sikter til. Likevel har jeg en frihet som jeg ikke hadde hatt om avhandlingen var skrevet på oppdrag fra arbeidsplassen min.

3.3 Forforståelse

Jeg hadde antakelser i oppstarten av dette prosjektet som jeg har vært svært bevisst på å lete like mye etter avkreftelse av som bekreftelse på. Noe har jeg fått bevist, andre ting er motbevist, og jeg håper det betyr at jeg har klart å møte eget felt med åpenhet. Underveis i oppgaven vil det presiseres hva som er bekreftet og hva som er avkreftet.

Tesen for oppgaven sier noe om min forforståelse.

- Det foreligger risikoer i dagens straffesakssystemer som gjør at politiet får vanskeliggjort sin arbeidssituasjon. Risikoene kan i tillegg påvirke publikum og svekke deres tillit til politiet.

Forforståelsen gikk altså først og fremst på at kvaliteten til straffesakssystemene ikke holdt mål. Jeg antok at rettssikkerheten var svekket som følge av situasjonen, og at publikums tillit kunne vært høyere om politiet hadde bedre straffesakssystemer. Den første delen mener jeg å ha fått bekreftet i aller høyeste grad, men det betyr ikke at resten av min forforståelse var korrekt. Jeg har til dels motbevist at rettssikkerheten svekkes og at publikums tillit er lav, men med noen modifikasjoner.

3.4 Forskningskrav

Alver og Øyen (1997) minner om det økende antall lover og retningslinjer som setter krav til forskere. De skriver at teknologi gjør informasjon lettere tilgjengelig og at det derfor stiller strengere krav til personvern enn tidligere. Dette er krav jeg må følge i mitt prosjekt. Jeg har

ikke hentet inn personinformasjon fra datasystemene, men har derimot sett på hvordan systemene fungerer, hvordan de brukes, hva slags type informasjon som lagres osv. Jeg har ikke brukt taushetsbelagt informasjon fra systemene og det har derfor ikke vært nødvendig å søke om tilgang til taushetsbelagt informasjon.

Anonymitetskravet (Alver og Øyen, 1997: 120-121) er oppfylt slik at informantene ikke kan gjenkjennes. Jeg har ikke samlet inn direkte personidentifiserende opplysninger om informantene, men deres arbeidssted, ansvarsområde og arbeidsoppgaver kan være indirekte personidentifiserende. Forskningsprosjektet er derfor meldt til Norsk samfunnsvitenskapelig datatjeneste og er godkjent derfra (vedlegg 6).

Et annet krav for forskningsprosjekter er kravet om informert samtykke (Alver og Øyen, 1997: 102). Alle informantene ble informert skriftlig, før intervjuet, om prosjektet og hensikten med forskningen. Prosjektet har endret seg noe underveis, men ikke mer enn at den informasjonen informantene har fått fortsatt er gyldig (vedlegg 5).

Videre skriver Alver og Øyen (1997: 29) at forskeren stilles til ansvar, særlig hvis funnene mislikes. Jeg er forberedt på at enkelte kan reagere på det jeg presenterer. Det er kanskje ikke ønskelig for alle at alt skal publiseres. Samtidig er det desto viktigere at forskningen gjennomføres da den skal gi grunnlag for utvikling og ny kunnskap.

3.5 Fra intervju til analyse

Om forskningen er troverdig vurderes ut ifra kvaliteten på dataene og om datainnsamlingen er utført på en tillitvekkende måte. Forskeren må argumentere for troverdigheten ved å informere om hvordan datainnsamlingen har foregått, hvordan dataene er analysert og dermed verdien av resultatene (Thagaard, 2006: 178). For å styrke troverdigheten av mitt prosjekt er det blant annet viktig å si noe om utvalget av informanter, både antallet, hvordan de aktuelle ble valgt, relasjonen mellom dem og meg, samt hvordan intervjuene er gjennomført. For å få svar på forskningsspørsmålene har jeg valgt å ha semistrukturerte intervjuer av strategisk utvalgte informanter. Følgende personer er intervjuet:

- En ansatt i PDMT som jobber med utvikling og endringer i straffesakssystemene. Heretter kalt systemspesialist.
- En representant fra MERVERDIprogrammet som har lang fartstid fra flere ulike roller i politiet. Heretter kalt straffesaksekspert.
- En sivilt ansatt som bruker straffesakssystemene i sitt daglige arbeid til søk og registrering. Heretter kalt bruker.
- En jurist som kan mye om straffesakssystemene sett opp imot lovverket. Heretter kalt jurist.

Om størrelsen på utvalget er tilstrekkelig kan diskuteres, da det er begrenset hvor dekkende fire personers meninger kan generaliseres til å være et uttrykk for politiet generelt. Gjennom dette utvalget håper jeg likevel å ha identifisert sentrale risikofaktorer ved og mulige konsekvenser av dagens straffesakssituasjon og det har vært det viktigste for meg. Ingen av informantene er politiutdannede. Det kan tilsynelatende virke som en mangel, men jeg har vurdert utvalget til å dekke det jeg er ute etter, fordi en politiutdannet ikke vil kunne gi meg informasjon om systemene som de utvalgte informantene ikke kan gi. Informantene har ulike posisjoner i politisystemet, ulik erfaring og kompetanse. Målet har vært at disse personene til sammen kan svare på forskningsspørsmålene og bidra til gode funn. Det kunne vært interessant å intervjuere personer i andre stillinger også, som for eksempel politikere og flere brukere, både politi og sivilt ansatte, men dette er ikke gjort primært av ressurs hensyn. De utvalgte informantene har ulike roller i straffesakssystemet som gjør at jeg får et bredt bilde ved å intervjuere akkurat de fire. Både det juridiske og historiske dekkes, samtidig som jeg får informasjon fra de som kan systemene best både teknisk og bruksmessig. Informantene er også på ulike nivåer i organisasjonshierarkiet. Det er ikke mange personer som sitter på akkurat den kunnskapen jeg har vært ute etter. Det er ikke mange i politiet som har inngående kunnskap om MERVERDIprogrammet, det er ikke mange jurister som har særskilt kunnskap om politiregisterloven og det er heller ikke mange som er spesialister på straffesakssystemene. Brukerkunnskap er det derimot mange som har, men også her er det store variasjoner i kunnskapens bredde og tyngde. Brukeren jeg har intervjuet har mange års erfaring fra ulike arbeidsplasser og med ulike arbeidsoppgaver.

Det er viktig å si noe om hvordan de aktuelle informantene ble valgt ut fordi jeg jobber i politiet selv. To av dem kjente jeg fra før og visste derfor at de satt med relevant kompetanse. Disse tok jeg direkte kontakt med. Den tredje ble jeg tipset om som relevant av en kollega. Denne introduserte oss via e-post. Den siste informanten kom jeg i kontakt med etter å ha gått gjennom mange ledd. Det var vanskeligst å få en informant ved PDMT, men det ordnet seg etter bistand fra min veileder Liv Finstad.

De to informantene som jeg hadde en relasjon til fra før intervjuene kjenner jeg gjennom arbeidsplassen min. Den ene er tidligere kollega, den andre er nåværende kollega. Jeg ville helst ikke intervju personer jeg kjenner fordi kjennskapet kan påvirke intervjusituasjonen og svarene jeg får. Informantene kan føle seg presset til å samtykke, og det kan være vanskelig å skille mellom hva som sies i fortrolighet og hva som er en del av intervjuet (Alver og Øyen, 1997: 131-132). I de to tilfellene hvor jeg hadde en relasjon til informantene fra før vurderte jeg relasjonen til at den ikke vil påvirke intervjuene i negativ retning. Denne vurderingen gikk på at informantene og jeg ikke har/hadde de samme arbeidsoppgavene eller bakgrunn. De har en annen bakgrunn og det er dermed ikke gitt at de mener det samme som meg. Det er også personer som er eldre og mer erfarne enn meg og jeg tror derfor ikke at mine meninger vil påvirke dem eller at de føler at de må svare i en viss retning. I tillegg var jeg svært bevisst på å minne om at jeg, under intervjuet, var student og ikke kollega.

Informanten jeg omtaler som *bruker* har jobbet i politietaten i 7 år og bruker de aktuelle systemene daglig, bortsett fra BOT. Juristen har vært i etaten i fem år, bruker ikke systemene mye, men har mye kunnskap om politiregisterloven og tilhørende forskrift.

Straffesakseksperten har jobbet i etaten i 26 år, er jurist, har erfaring med systemene som bruker og er nå dypt inne i arbeidet med å lage nye straffesakssystemer. I tillegg har vedkommende mye ledererfaring. Systemspesialisten har vært i politietaten siden 1988, og i PDMT siden 2006. Personen har lang erfaring som bruker av systemene før vedkommende ble spesialist i PDMT.

En av informantene sitter i RESP, en er ansatt i POD og en i Kripos, uten at jeg vil informere hvem som er hvem fordi denne informasjonen kan bidra til personidentifisering. Poenget er at alle informantene har lang erfaring og mye kunnskap om straffesakssystemene, men fra litt ulike ståsteder.

Alle intervjuene har foregått på arbeidsplassen til informanten, enten på kontoret eller på et møterom, og de varte omtrent to timer. Som Thagaard (2003: 86) skriver er det viktig at forskeren setter seg inn i informantens situasjon i forkant av intervjuene slik at spørsmålene synes relevante for informanten. Samtidig er det viktig å stille spørsmål som inviterer til refleksjon. Jeg hadde forberedt spørsmål til intervjuene som jeg ønsket å få svar på. Samtidig forsøkte jeg å være åpen og mottakelig for at informanten kunne sette fokus på andre elementer enn det jeg forventet og ønsket. Jeg hadde en intervjuguide, men den ble ikke fulgt slavisk. Intervjuguiden var heller ikke lik for de fire informantene. Spørsmålene var laget med tanke på den enkelte informants rolle og/eller kunnskap om straffesakssystemene. Jeg forsøkte å lytte, stille relevante oppfølgingsspørsmål og vise at jeg forstod svarene ved å forklare hvordan jeg oppfattet det informantene sa.

Fra før hadde jeg lite erfaring med å intervju, det var derfor en utfordring å få til gode intervjuer, men jeg er fornøyd i etterkant. Informantene uttrykte også at de synes det var interessant å snakke med meg. En av informantene uttrykte at intervjuet gav tid til å reflektere på en annen måte enn det som ble gjort i hverdagen og så nytten i det. Alle informantene tilbød ytterligere kontakt eller flere intervjuer om det ble nødvendig.

Jeg opplevde atmosfæren i alle intervjuene som trygg og tillitsfull. Informantene snakket fritt og åpent, det virket ikke som om de holdt tilbake informasjon og heller ikke som om de delte mer enn de hadde lov til. Av og til la de til grunn at jeg visste hva de snakket om ved å si «...ja det kjenner jo du til...» eller «...dette vet jo du alt om». I de tilfellene det skjedde ba jeg informantene utdype hva de mente. Under analysen har jeg bevisst prøvd å legge til side min bakgrunnskunnskap og konsentrert meg kun om det informantene sa.

Mot slutten av arbeidet med oppgaven så jeg noen ting jeg kunne gjort annerledes som jeg drar lærdom av. Under intervjuene snakket vi mye om begreper som jeg definerer i oppgaven, for eksempel risiko, rettssikkerhet og tillit. Jeg spurte dessverre ikke informantene hvordan de ville definere begrepene eller hva de la i de ulike begrepene. Den informasjonen kunne gitt meg mye informasjon og bidratt til at eventuelle tolkningsfeil ville vært unngått.

En annen ting jeg så tydelig da jeg transkriberte intervjuene var min og informantens felles forståelse for at temaet var noe jeg kunne mye om fra før. Derfor ble inngående forklaringer av systemenes funksjoner og oppbygging utelatt selv om det kunne vært interessant. Selv om informantene visste at jeg hadde bakgrunnskunnskap om temaet var jeg ute etter hva de mente

og visste. Jeg ba dem snakke til meg som om jeg ikke hadde bakgrunnskunnskap om temaene, men dette kunne jeg også presisert utover i intervjuet og jeg kunne spurt mer inngående om systemene. I stedet ble det innforstått at vi hadde felles forståelse av dette. Jeg kunne også stilt flere oppfølgingsspørsmål. Jeg tror ikke jeg har gått glipp av avgjørende informasjon på grunn av dette, men jeg vet ikke om det er noe informantene og jeg oppfatter ulikt selv om vi tilsynelatende hadde samme forståelse.

Relasjonen til informanten endrer seg fra datainnsamlingen til analysen og tolkningen (Thagaard, 2006: 14). Under intervjuet har informanten kontroll ved at han eller hun styrer hva som blir sagt, men under analysen bestemmer forskeren hvordan informanten skal presenteres (Thagaard, 2006: 106). Jeg har skrevet en temasentrert oppgave, noe som innebærer at jeg har sammenlignet temaene informantene snakket om, i motsetning til å sammenligne informantene i seg selv eller deres historier. Ifølge Thagaard (2006: 167-168) kan dette være etisk problematisk, fordi informantene kan oppleve det som presenteres som oppstykket og tatt ut av sammenheng. Informantene ble informert om temaene underveis i intervjuene, men likevel er det transkriberte intervjuet stykket opp og spredd ut igjen gjennom min tolkning. Sånn må det bli i en temasentrert forskningsoppgave og jeg er trygg på at jeg ikke har tillagt noen av informantene noe de ikke har sagt. Det er ikke usannsynlig at min forskningsforståelse er annerledes enn informantens forståelse av straffesakssituasjonen, men jeg har forsøkt å skille mellom informantens utsagn og hvordan jeg har tolket det de sa under intervjuene. For å tydeliggjøre dette skillet har jeg gjengitt en del sitater, for deretter å komme med min tolkning. Dermed kan leseren fritt vurdere min tolkning. I tilfeller hvor det ikke presiseres hvor informasjonen er hentet fra, eller hvorvidt det er min eller informantens mening, så er det informantens mening. Det er ikke nødvendigvis et faktum som politietaten som helhet stiller seg bak.

Under analysen skal forskeren knytte dataene til annen forskning og relevante teoretiske perspektiver. Forskerens ståsted og bagasje vil da tre inn og påvirke tolkningen av innsamlet data samtidig som informantens perspektiv skal bevares. I analysefasen tenkte jeg nøye gjennom hva informantene egentlig hadde sagt før jeg tolket det.

Analysen har ikke foregått som en isolert del av prosjektet. Datamaterialet ble analysert helt i fra begynnelsen og underveis i skrivingen. Formidlingsformen kan også forstås som en del av

analysen. Under analysearbeidet delte jeg datamaterialet i matriser med ulike fargekoder for å visualisere temaene og tendensene. Denne metoden gjorde det lett for meg å se likheter og forskjeller mellom de ulike informantenes forståelse. Matrisene hang på veggen på kontoret mitt under hele prosessen. Dermed bidro matrisene til at jeg hele tiden så grunnlagsmaterialet mens jeg utviklet analysen.

Bekreftbarhet går på hvordan resultatene tolkes, altså kvaliteten av tolkningen. Det innebærer forskerens evne til å være kritisk til egne tolkninger og om det finnes annen forskning som kan støtte resultatene (Thagaard, 2006: 179-180). Målet mitt har vært å levere et solid forskningsmateriale. Derfor har jeg hele tiden forsøkt å være kritisk til funnene og tolkningen av disse. Thagaard (2006: 180) foreslår å bruke andre til å se svakheter ved egne refleksjoner. Hun sier også at det er nyttig å prøve ut alternative tolkninger. Disse rådene har jeg forsøkt å følge. Jeg har fått kolleger, venner og medstudenter til å lese og kommentere underveis.

Jeg har sett på det innsamlede datamaterialet i et risikoperspektiv, noe som ikke var helt klart fra begynnelsen av prosjektet. De to første intervjuene som ble gjennomført hadde ikke så mye vekt på risiko som de to siste intervjuene hadde. Likevel er alle intervjuene analysert med den samme vekten på risikoteori. Jeg mener at jeg har klart dette uten å tillegge eller trekke noe vekk fra informantenes bidrag.

3.6 Forskningsresultatenes overførbarhet

Overførbarhet er når forskningsresultatene kan gjelde i andre sammenhenger selv om det er basert på en enkel undersøkelse (Thagaard, 2006: 21). Tolkninger kan bli testet og videreutviklet i nye forskningsprosjekter. Spørsmålet er om de teoretiske konklusjonene jeg trekker også kan settes i en videre sammenheng?

Jeg vil ikke trekke den konklusjonen at politiet ikke risikovurderer noen av sine IKT-systemer eller andre områder i politiet, selv om jeg har funnet ut at de ikke risikovurderer straffesakssystemene. Ett av målene ved prosjektet å bidra til at feil som finnes i dagens straffesakssystemer ikke gjentar seg i nye systemer. Prosjektet kan bidra til dette ved å peke

på hvilke vurderinger som tas i dag når det gjelder risiko og utvikling av IKT og hva vurderingene har ført til.

Jeg mener oppgaven kan gi kunnskap om risikoer og vurdering av risiko i politiet. Dagens situasjon er et eksempel på hva som kan skje når risiko ikke blir vurdert. Derfor kan fenomenet ha overføringsverdi til andre organisasjoner eller temaer. Selv om denne studien baserer seg på kun fire intervjuer, er det mulig å gyldiggjøre fenomenet i en større sammenheng. Politiet kan lære av andre organisasjoners suksesshistorier. På samme måte kan andre organisasjoner lære av politiets manglende risikostyring. I avslutningskapittelet presenterer jeg forklaringskjeder som kan forklare hvordan politiet kan oppnå bedre resultater.

3.7 Å skrive om et tema i forandring

De to siste årene har vært alt annet enn *business as usual* for norsk politi. Etaten har vært i en stor omveltningssprosess og er det fortsatt. Det å skrive om et tema som er så dagsaktuelt har vært utfordrende. Det skjer mye på to år. Dermed kan det jeg skriver om stille seg helt annerledes fra en dag til en annen.

På mange måter begynte den store omveltningen med rapporten fra 22. juli-kommisjonen. Deretter kom Politianalysen. Midt oppi det hele har det vært regjeringsskifte og omorganiseringer i politiet. Utviklingen av nye straffesakssystemer har satt fart, Politidirektoratet opprettet en egen IKT-avdeling i slutten av 2013, ikrafttreddelsen av politiregisterloven nærmer seg og den politiske styringen har endret seg. Notater fra en dag er ikke lenger relevant dagen etter, ting forandrer seg og noe viser seg å ikke lenger være aktuelt. De intervjuedes rolle i etaten har også endret seg. Lovverket har endret seg, den politiske prosessen har endret seg. At IKT er mer prioritert er nytt. Midt oppi dette har jeg forsøkt å skrive noe fornuftig om det som er, det som skjer og det som kommer. På den måten skrives et lite stykke historie og mitt ønske er at det kan brukes til noe fornuftig.

4. Straffesakssystemene

I dette kapitlet presenteres det informantene valgte å trekke frem som risikoelementer knyttet til straffesakssystemene. Politiet vet mye om hvilke risikoer som kan oppstå, men så vidt jeg har forstått er det ikke utført systematiske risikoanalyser av kvaliteten på straffesakssystemene. Jeg skal drøfte risikoenes betydning for politiets oppgaveløsning og hvordan risikoene kan påvirke rettssikkerheten for de registrerte og publikum.

4.1 Risikovurderinger

I dagens vestlige samfunn er det vanlig å være redd for å bli et offer. Avvik blir sett på som kilden til risiko. Risikosamfunnet har et negativt fokus på det farlige istedenfor å fokusere positivt på det gode. Det ligger en kollektiv frykt mot det ukjente og farlige, og det er en felles oppfatning om at samfunnet er utrygt. Derfor kreves det mer kunnskap om risiko som igjen skaper enda mer å være redd for. På denne måten produseres farlighet (Ericson og Haggerty, 1997: 6). Det etterstrebes nok kunnskap til å kunne beskytte seg, men det er vanskelig å vite hvor kunnskapsnivået bør stoppe. Risikosamfunnet er et kunnskapssamfunn hvor ønsket er mer kunnskap om det som utgjør risiko. IKT har hatt stor betydning for hvordan det er mulig å sette opp risikoanalyser. Hvordan risikoanalyser gjennomføres sier noe om en institusjon (Ericson og Haggerty, 1997: 8-9).

Luhman skriver at vi vurderer sosiale og materielle konsekvenser i forkant av en beslutning (Luhman, 1993: 37). Vurderingen av en hendelse er ofte annerledes i forkant enn i etterkant, selv om hendelsen er et resultat av vurderingen som ble gjort i forkant (Luhman, 1993: 16). Da jeg startet på denne oppgaven hadde jeg forventet å få bekreftet at politiet har foretatt risikovurderinger av kvaliteten på straffesakssystemene, men det gjorde jeg ikke. Jeg fant heller ingen systematiske kartlegginger av hvilke risikoer som er knyttet til systemene og hva som kan skje dersom risikoene slår ut. Verken brukeren, juristen eller straffesakseksperten kunne vise til risikovurderinger av systemene, men alle mente det ville være interessant lesning. Det er forunderlig at det ikke finnes helhetlige og systematiske vurderinger av hvilke risikoelementer som er knyttet til straffesakssystemene, hvilke konsekvenser som kan inntreffe og sannsynligheten for dette. Fraværet av risikoanalyser er i strid med hvordan risikoteoretikerne hevder at risikosamfunnet forholder seg til risiko. Som beskrevet i kapittel 2

forholder vi oss til risiko hele tiden. Dermed kan det antas at politiet har en uformell og ustrukturert tilnærming til risiko. Tore Hartvigsen skrev i 2013 en masteroppgave om risikoanalysemetoder for å håndtere risiko i det moderne informasjonssamfunn. Han gjennomgår en rekke eksempler fra store organisasjoners informasjonssystemers rolle i større ulykker, deriblant politiet og 22. juli. Hartvigsen konkluderer med at risikoanalyser ikke har blitt tilstrekkelig gjennomført eller ikke er utført i det hele tatt (Hartvigsen, 2013: 5). Åtte eksempler på ulykker hvor menneskeliv har gått tapt gjennomgås av Hartvigsen og han viser at politiet ikke er alene om å ikke risikovurdere egne systemer:

Mest sannsynligvis var ikke informasjonssystemene gjenstand for egne risikogjennomganger i de ulykkene som er gjennomgått. Det er ikke funnet noen omtale av utførte risikogjennomganger verken i rapportene fra de bransjer hvor dette tradisjonelt gjøres, eller i noen av de andre rapportene som er gjennomgått (Hartvigsen, 2013: 70).

Det må presiseres at politiet har utarbeidet rapporter om politiets behov, mål og krav i forbindelse med utviklingen av nye straffesakssystemer. Disse har imidlertid hverken innhold eller metodikk som en risikoanalytiker vil definere som en risikoanalyse. Det er ikke definert hva som anses som risikomomenter, hvilke konsekvenser som kan oppstå eller sannsynligheten for dette. Fokuset har vært på hva nye systemer må inneholde av funksjoner. Dagens systemer skal fungere i flere år fremover, og det kunne derfor vært nyttig å vurdere og styre risikoen vedrørende dem. En rapport skrevet av Accenture (Accenture-rapport, 2010) fastslår at IT-funksjonene i politiet har høy risiko. Påstanden er ikke basert på risikoanalyser av systemene, men en gjennomgang av PDMT.

Nåsituasjonen er vurdert i forhold til Accentures IT Capability Maturity Model (IT CMM). Modellen er utviklet av Accenture basert på erfaring hos kunder over hele verden, og inneholder en detaljert beskrivelse av evner eller egenskaper en IT organisasjon må ha for å kunne levere moderne IT tjenester (Accenture, 2010: 2).

Denne rapporten kommer jeg tilbake til flere ganger underveis.

I tabell 5 i en *Kvalitetssikringsrapport* (2013: 32-34) som kvalitetssikrer MERVERDIprogrammet står det at det er påbegynt et arbeid med å etablere metoder for risikovurdering og at nivå for akseptabel risiko diskuteres. Når dette er avklart skal det implementeres lokalt. Dette er risikovurderinger av informasjonssikkerheten, og angår ikke mitt undersøkelsesområde som er kvaliteten på straffesakssystemene. I tabell 6 i samme rapport står det at det ikke gjennomføres sentrale risikoanalyser i politiet, men det jobbes med

å få det etablert. Igjen er det snakk om informasjonssikkerhet. Som sagt betyr ikke dette at politiet ikke kjenner til noen former for risiko eller at de ikke har dokumentert sine behov. MERVERDIprogrammet er et resultat av en lang prosess mot nye straffesakssystemer. Straffesakseksperten fortalte at konseptvalgutredningen ble ferdigstilt i november 2011. I denne ble det lagt frem tre alternativer for hvordan straffesakssystemene kunne bedres. Alternativet *Nybygg* ble anbefalt på bakgrunn av behovene til politiet. Sommeren 2012 sa politikerne ja til dette alternativet. *Nybygg* var det dyreste alternativet. Det medfører en total fornyelse av straffesakssystemene hvor alt skal bygges opp på nytt. De to andre alternativene ble sett som oppussing av eksisterende systemer. Alternativet som medførte færrest endringer og hadde lavest kostnad ble kalt for *Null-alternativet*. Det siste alternativet lå mellom de to andre og ble kalt *Modernisering*. I forbindelse med utarbeidelsen av disse alternativene ble risikoen ved å ikke gjøre noen ting med straffesakssystemene vurdert. Straffesakseksperten sa at den vurderingen bidro til at det ble bestemt å gå for det mest omfattende alternativet. Videre fortalte straffesakseksperten at MERVERDIprogrammet ikke foretar andre risikovurderinger enn det de gjør av eget arbeid: «Våre risikovurderinger knytter seg til om vi får det til eller ikke, men risikoprofiler knyttet til om det stopper opp eller ikke er ikke vårt mandat», og informanten henviste videre til PDMT. Systemspesialisten fortalte at de har to leveranser i BL og Strasak i året. I forkant av leveransen vurderes risiko av det som skal leveres. Det er en teamleder som tar initiativ til hva som må risikovurderes. Deretter samles hele teamet for en analyse av hendelser som kan oppstå. Det som vurderes da er hvilke tekniske følgefeil som kan oppstå i forbindelse med leveransen. Vurderes en leveranse til å ha risiko for tekniske følgefeil kan leveransen midlertidig stoppes og ytterligere testing foretas før eventuell ny leveranse. Da finner de alternativer, tester det og risikovurderer på nytt til risikoen er på et akseptabelt nivå.

Det er altså ikke foretatt risikovurderinger av straffesakssystemene, men når jeg ba informantene fortelle om dagens situasjon, problemer, utfordringer og risiko hadde alle mye å fortelle selv om de vektla til dels ulike ting. Noen problemer er større enn andre og informantene hadde ulik oppfatning av hvor stor risiko utfordringene utgjør. Videre i kapitlet blir det en gjennomgang av risikoene informantene fortalte om og konsekvensenes omfang. I konseptvalgutredningen ble dagens situasjon beskrevet, og det gir et bilde av det samme som informantene fortalte:

Dagens straffesakssystemer kan sies å ha åpenbare svakheter, f.eks. knyttet til manglende funksjonalitet til å dele informasjon på tvers av politidistrikter. Samtidig er det funksjonalitet som savnes av politiet og som kan redusere mengden av manuelt arbeid og dobbeltregistrering. Teknisk er løsninger delvis ustabile og IKT-situasjonen er generelt preget av forvaltningsetterslep og fragmenterte systemer. Det er i dag ikke støtte for ny straffelov (KS1 konseptvalg 2012: 17).

4.2 Driftsavbrudd og kollaps

Gamle og fulle systemer utgjør en risiko for driftsavbrudd og i verste fall kollaps.

Systemspesialisten fortalte at en risiko knyttet til straffesakssystemene er at de er gamle og fulle. Systemene består av moduler. Hver gang noe endres lages en ny modul. Til slutt er det fullt. Det skaper risiko for tekniske feil, feil opplysninger og andre ukjente følgefeil. Et eksempel på en feil som PDMT ikke kan forklare er at tekst forsvinner i BL. Når lange avhør eller anmeldelser er skrevet blir plutselig alt som er skrevet borte. Av de ulike risikoene som presenteres i dette kapitlet er driftsavbrudd og tekniske feil i systemene kanskje den risikoen som påvirker politiets arbeid mest i det daglige. Den tiden et system er ute av drift kan skape frustrasjon og stress for brukerne. Når det oppstår tekniske feil, brukes det mye tid på å rette opp og finne ut av feilen. Tiden som forsvinner her er tid som kunne og skulle vært benyttet til viktig arbeid med politiets oppgaveløsning innen straffesaker. Selv korte tidsavbrudd kan påvirke effektiviteten og muligheten for å tilrettelegge egen arbeidsdag, men når et system først er nede går det gjerne litt tid før det fungerer igjen. Som nevnt over kan det også være at utført arbeid forsvinner og må gjøres på nytt. Systemspesialisten fremhever at PDMT ofte kan gjenopprette tapt informasjon og at de driver kontinuerlig utviklings- og vedlikeholdsarbeid. Som jeg nevnte over har PDMT to leveranser i året hvor de foretar endringer og forbedringer i BL og Strasak. Endringene er etter ønsker fra brukerne, eller etter eget initiativ. Det er en fagansvarlig som tar beslutninger når det gjelder prioritering av endringsforslag og i hvilken rekkefølge feil skal rettes. Gjennom dette arbeidet blir BL og Strasak bedre, men det er ikke mulig å gjøre forbedringer i det uendelige da systemene blir fulle. Slik jeg oppfatter systemspesialisten kan straffesakssystemene sees som et puslespill. Puslespillet blir bedre og bedre ettersom nye brikker legges til, men til slutt blir det fullt og brikkene går utenfor puslespillets rammer. Da skapes risiko for at alt bryter sammen.

Juristen uttrykker usikkerhet når det gjelder om situasjonen egentlig er så dramatisk og lurer på hva som skjer hvis det i verste fall går galt og noen systemer kneles. Ifølge systemspesialisten kan det skje. I Accenture-rapporten (2010: 12) står det at det finnes kriseplaner dersom noe skulle gå galt, men Accenture vurderer likevel risikoen som høy. Systemspesialisten fortalte videre om risikomomenter ved Strasak. Strasak kjøres fra en såkalt stormaskin som står på PDMT og informanten sa: «Vi har jo stormaskinen her, og så lenge Strasak går, må stormaskinen leve og det er sårbart, det er gammelt. Vi leier inn utviklere, de er over 60 år alle sammen og de er de eneste som kan dette her. Vi trenger de for å drifte og supportere.» Kneles maskinen er det full stopp, -og det kan ikke registreres noe inn via BL, statistikker kan ikke tas ut, heller ikke bøteattester. Informanten sa at det er fatalt hvis noe skjer med stormaskinen. Videre sa informanten: «Det har ikke vært lett å få tak i rett folk. Det er en utdøende rase, det er det. Så finner vi noen og er heldige, det redder oss. Det er jo også en risiko. Sånn er det nå en gang.» Dette er et eksempel på at politiet arbeider erfaringsbasert og ikke kunnskapsbasert. Det viser også at kunnskapen om systemene er i ferd med å forsvinne og det er ikke satt inn tiltak for å føre kunnskapen videre. Dette kommer jeg tilbake til i kapittel 4.6.

Ut i fra dette kan en påstå at det er risiko for at det vil ta tid før stormaskinen er reparert om den skulle knele. I den tiden maskinen er ute av drift er det ingen andre løsninger for de arbeidsoppgavene Strasak brukes til. Dermed kunne en tro at politiet ikke er så avhengig av Strasak, men det er mange oppgaver som ikke kan utføres når systemet ikke fungerer.

Systemspesialisten kunne fortelle at BOT delvis er faset ut nettopp fordi systemet var gammelt og fullt. Av den grunn forelå det høyrisiko for at systemet skulle knele. BOT ble faset ut før det kollapset. Strasak har ikke kollapset enda, men det kan skje, ifølge systemspesialistens beskrivelse av stormaskinen. Om det skjer får det store konsekvenser. At systemspesialisten fortalte at det forelå høyrisiko for at BOT kunne knele vitner om at systemet har vært risikovurdert, men systemspesialisten sa at det kun risikoanalyseres i forbindelse med leveranser.

I og med at BOT er faset ut går opplysningene som tidligere gikk fra BL til BOT, nå fra BL til Strasak. Bøteattester bestilles gjennom statistikkprogrammet PAL. Informanten fra PDMT sa at det fungerer utmerket og at det er planer om at straffeattester fra SSP også skal bli mulig å hente ut ifra PAL. Straffesakseksperter fortalte at dagens straffeattester ser gammeldagse ut

og er uoversiktlige fordi SSP er et gammelt system. Blant annet er alt i SSP skrevet med store bokstaver, noe annet er ikke teknisk mulig, og på grunn av plassmangel for fritekst er det mye bruk av forkortelser. Plassmangelen for fritekst er en teknisk begrensning angitt av systemet og kan ikke endres på. Disse to tingene, i tillegg til et gammeldags brukergrensesnitt basert på DOS, gjør at det ser gammeldags og uoversiktig ut. På hjemmesidene til *Norsk datakunnskap network* står det at DOS ikke støtter multitasking, mens Windows er et mer avansert og brukervennlig operativsystem som støtter multitasking. Etersom straffesakssystemene baserer seg på DOS er de ikke tilrettelagt for å håndtere flere operasjoner på en gang og effektiviteten hemmes.

Accenture-rapporten (2010) viser at PDMT har et unormalt lavt kostnadsnivå sammenlignet med andre IT tjenesteleverandører av samme størrelse. Grunnen til dette er at det ikke stilles høye krav til kvalitet og at det er aksept for høy risiko i det PDMT leverer. I rapporten konkluderes det med at det er stadig økende operasjonell risiko og brukerne er lite tilfredse (Accenture-rapport, 2010: 10). Den høye operasjonelle risikoen skyldes manglende styring, kontroll og overvåking av produksjonsmiljøet. En utfordring for PDMT er at det ikke finnes ett system som overvåker løsninger i drift og fanger opp driftsavbrudd, feil, kilder til feil eller konsekvensene av feil. Det avhenger av den enkelte ansattes innsikt og fange opp omfanget av slike forekomster (Accenture-rapport, 2010: 19). Den høye operasjonelle risikoen skyldes også foreldet infrastruktur og applikasjonsportefølje og for lite finansiering til vedlikehold. Det viser seg at PDMT ikke har gode rutiner for testing, kvalitetssikring og produksjonssetting. For å nå tidsfrister og/eller kostnadsbegrensninger, hender det at løsninger produseres uten at det er tilstrekkelig testet. Det mangler også på risikovurderingsprosesser og iverksettelse av korrigerende tiltak. Alt dette til sammen viser at det er høy sannsynlighet for feil og driftsavbrudd i politiets systemer (Accenture-rapport, 2010: 12). Accenture vurderer risikoen til å være høy også når det gjelder mangelfull planlegging for når systemer skal fases ut eller oppgraderes.

4.3 Kodeverk, ulik registreringspraksis og statistikk

Straffesakssystemenes lave brukervennlighet og kodeverk utgjør en risiko for at ulike politidistrikter legger seg på forskjellig registreringspraksis. Problematikken belyses i politianalysen:

Politiets ulike registre føres i det vesentlige lokalt ved det enkelte politidistrikt/særorgan uten klare nasjonalt forankrede rutiner for registrering av opplysninger. Vi har erfart at politidistriktene operer med ulike rutiner for bl.a. prioritering av operative oppgaver i PO, og bruk av avgjørelseskode i Strasak, noe som gjør det krevende å gjøre sammenlikninger mellom politidistriktene (Politianalysen, 2013: 246).

I sitatet over henvises det til ulike rutiner for bruk av avgjørelseskoder. En avgjørelseskode forteller hvordan en sak er avgjort. Hvis en sak henlegges, har politiet mange alternative henleggelsesårsaker og henleggelseskoder. Flere av kodene har glidende overganger, og så lenge det ikke er innarbeidede sentrale rutiner for bruken av dem kan det fort bli ulik lokal praksis for hvilke koder som benyttes i de ulike distriktene. To tilsynelatende like saker som henlegges av samme grunn, kan altså bli registrert med noe ulik avgjørelseskode.

Konsekvensene er at det blir rotete, vanskeligere å gjenkjenne samme avgjørelse og feil i statistikken. To ulike henleggelseskoder kan også være bestemmende for om informasjonen må slettes fra systemene eller ikke.

Ulik praksis rundt registrering kan også tyde på to andre elementer. Det kan være at lovverket er uklart og/eller at rutinene ikke samsvarer med lovverket. Jeg har ikke undersøkt politiets praksis med utarbeidelse av rutiner opp imot lovverk, men informantene fortalte at den juridiske opplæringen for brukerne ikke alltid er så sterkt vektlagt. Her siktes det til opplæringen som foregår på arbeidsplassen og ikke opplæringen som gis på Politihøgskolen.

Meg: Får de som bruker systemene juridisk opplæring? Da tenker jeg innen personvern, strafferett, forvaltningsrett, informasjonssikkerhet osv.?

X: Ja, men det har vært varierende. Man er flinkere til det nå. Hvor systematisk det er, er jeg usikker på. Det er sånn overordnet. Jeg vet ikke om det er praksis i distriktene, det tror jeg ikke.

En klassisk diskusjon i politisosiologien går på balansegangen mellom legalitet og effektivitet, om politiet ser seg selv som rettslige aktører eller håndverkere. «Dilemmaets kjerne sett fra politiets ståsted er at politiet forventes å være effektive kriminalitetsbekjempere samtidig som politiet skal ivareta rettssikkerheten» (Finstad, 2013: 130). Hvis den juridiske

opplæringen ikke vektlegges i særlig grad, blir det opp til hver enkel å sette seg inn i rettsreglene. Det betyr at det ikke blir en enhetlig praksis, men ulike rutiner. På den måten går håndverkerdimensjonen eller effektiviteten foran legaliteten. På den andre siden kan ulik praksis skape usikkerhet blant de som skal utføre arbeidsoppgaven og dermed oppnå heller ikke effektivitet. Som Finstad skriver er det en balansegang mellom de to elementene hvor de må tilpasses hverandre. Som informantene vektlegger kan politiet oppnå mer av begge deler ved å gjennomgå og spisse sine rutiner opp imot lovverket, og dermed skape grunnlag for mer enhetlig oppgaveløsning.

Det er et krav til god statistikk at den er nøyaktig, pålitelig og etterprøvbare. Kodeverket utgjør en risiko for at statistikken ikke oppfyller kravene. Luhman skriver at koding av teknologiske systemer innebærer å legge inn verdier. Kodene er bindende og utgjør derfor en risiko. Mine informanter kan fortelle at det er utfordringer vedrørende kodeverket i straffesakssystemene særlig med tanke på statistikk. Både BOT, SSP og Strasak er grunnlagssystemer for uttak av statistikk. Informantene fortalte at det hender at det er teknisk svikt når statistikken skal tas ut, men stort sett fungerer det. I de tilfellene det er teknisk svikt, kan statistikken utebli helt, men det tilhører sjeldenheten. Straffesakseksperten fortalte at det er kodene som legges inn i Strasak, for eksempel kodene for straffebud, som er problemet. Kodene må endres underveis i en sak hvis straffebudet endres. Hvis endringen ikke utføres står det i statistikken at saken gjelder noe annet enn det som er reelt. Ikke alle har like stort fokus på dette ifølge informanten, som også fortalte at Strasak metodisk sett ikke tilfredsstiller kravet til holdbar statistikk. Ifølge informanten er det prinsippet for etterprøvbarehet som mangler fordi man endrer kodene i Strasak stadig vekk. For å sikre en viss grad av etterprøvbarehet fryses Strasak 31.12 hvert år slik at det er mulig å gå tilbake og se historikken. Systemspecialisten sa ingenting om at statistikken ikke er etterprøvbare, informanten sa at ut av de opplysningene som ligger i Strasak er statistikken etterrettelig. Brukeren poengterer at statistikken ikke er pålitelig fordi kvaliteten på det som registreres inn er for dårlig. Ifølge informanten har juristene fokus på å bruke riktige koder, som for eksempel avgjørelseskoder, men det er ikke alltid juristene som gjør selve registreringsjobben. Den gjøres i mange tilfeller av andre sivilt ansatte, og registreringen slurves det noe med. Straffesakseksperten fortalte mer om koding i systemene:

En politistasjon i Oslo har 16 personer for å kode saker. Det er sivilt ansatte. Vi bruker masse ressurser på å legge dette inn og så er vi dårlige på gjenbruken av det tror jeg. Vi koder i forhold til straffebud, det er gammeldags. Vi kan bare ta ut statistikk på bruk av straffebud og parametere er saksbehandlingstid og prosent i forhold til frifinnelse eller ikke og hvor mange saker vi har og hvor mange i forhold til i fjor og sånn. Men det stemmer ikke fordi vi endrer jo Strasak underveis. Det er informasjonsflyten som starter med koding av saker som gjør at vi ikke får den informasjonen vi trenger for å løse saker ute. Dette er tatt opp i et mandat som justis gav oss for noen år siden. Vi lagde en tilstandsrapport av hva som ikke fungerte og der står det at det er til hinder for at vi kan gjøre jobben.

Det er altså behov for statistikk som gir mer informasjon utover registrerte straffebud. Systemspesialisten kan i tillegg fortelle at Strasak-kodeverket ikke samsvarer med kodeverket i andre systemer som for eksempel Elys, som er et etterlysningsregister. Systemspesialisten sa at når nye systemer kommer, blir det slutt på koding og det blir en ny måte å registrere på. Informanten opplyste å ikke ha ytterligere kjennskap om dette.

Når det gjelder kodeverket, er risikomomentet todelt. Det ene handler om at kodeverket ikke samsvarer med kodeverket i andre systemer og det andre handler om at de som registrerer og endrer gjør feil. Begge deler skyldes at systemet er dårlig tilrettelagt for brukerne og som statistikkgrunnlag. Det må uansett stilles krav til nye straffesakssystemer at de gir et bedre grunnlag for uttak av statistikk enn det som finnes i dag.

4.4 Ny straffelov

Tekniske svakheter i BL og SSP utgjør et risikomoment fordi det ikke er mulig å implementere ny straffelov. Systemspesialisten fortalte at både BL og SSP står i veien for ny straffelov på grunn av tekniske utfordringer. Systemene tåler ikke at det bygges flere moduler, noe som må til hvis nye typer lovbrudd skal leges inn. Legges det inn mer nå vil systemene kollapse. Informanten sa at det var for datateknisk komplisert å forklare utfordringen nærmere. Følgende står i straffeloven av 2005:

Loven er ment å erstatte nåværende straffelov fra 1902 (straffeloven 1902). Loven er vedtatt, men er ikke satt i kraft med unntak av kapittel 16 om folkemord, forbrytelse mot menneskeheten og krigsforbrytelse. Straffeloven 2005 i sin helhet vil ikke bli satt i verk før tidligst 2014. Politidirektoratet mener at straffeloven 2005 må legges inn i politiets datasystem før man kan begynne å bruke den. Årsaken til at den nye loven ikke kan tre i kraft i sin fulle bredde er p.g.a. politiets datasystem som først skal fornyes.

I forkant av prosjektet tok jeg det som en selvfølge at politiet har vært klar over problematikken med implementering av loven i straffesakssystemene, men straffesakseksperten fortalte at sammenhengen mellom IKT og ikrafttredelse av straffeloven ikke er oppdaget før nylig fordi politiet sitter på hver sin tue og ikke ser ut over eget ansvarsområde. Juristen fortalte at det er politisk press for at ny straffelov skal tre i kraft og at det derfor kan komme noen raske løsninger i dagens systemer. Systemspesialisten håper ikke det blir en realitet da det anses som meget teknisk utfordrende å møte kravene det medfører. Det foreligger altså en risiko både ved at loven ikke trer i kraft og hvis den trer i kraft før politiet har straffesakssystemer som kan håndtere endringene.

Normer, lover og økonomi har en historie bak seg og er tungt og avansert institusjonalisert i dagens samfunn (Luhman, 1993: 53). Hva som blir sett på som rett og galt skaper forventninger i en gitt tid. Så lenge det er enighet om en norm, mener Luhman at det ikke er noen risiko forbundet med handlingen og lover utgjør ikke en risiko fordi den tar fremtiden inn i nåtiden (Luhman, 1993: 55). I Norge har vi kommet i den situasjonen at borgerne er enig om at forandringer i samfunnet og den teknologiske verden har utviklet seg og at straffeloven må endres som en konsekvens av dette. Dagens straffelov er fra 1902 og det er derfor vedtatt en ny lov som tar høyde for de endringer som har skjedd i samfunnet slik at bestemmelsene blir mer tidsriktige. Den nye straffeloven åpner for eksempel for at terrorhandlinger kan straffes med fengsel inntil 30 år⁴. Dette er et eksempel på at samfunnet ser terror som en større risiko enn før. Etersom loven ikke har trådt i kraft, er samfunnets kontrolltiltak mislykket. Utfallet blir at borgerne ikke beskyttes mot overgrep fra den siktede i like stor grad som de ville blitt hvis den nye loven var trådt i kraft og straffen kunne vært skjerpet. Norge befinner seg derfor i en situasjon Luhman ikke diskuterer. Gjeldende lov er utdatert og tar ikke fremtiden inn i nåtiden, men utgjør isteden en risiko. Samfunnet er enige om normen, men det er likevel risiko forbundet med handlingen fordi straffemuligheten enten er for lav eller ikke tilstede. Bernt og Doublet (1999: 167-168) tolker Luhman sitt arbeid. De skriver at Luhman ikke ser retten som identisk med loven, men at retten er slik den praktiseres av de som anvender den uten påvirkning av politiske aktører. I den situasjonen Norge er i dag, er det andre elementer som påvirker både retten og loven, nemlig straffesakssituasjonen til politiet. Det er en situasjon som kanskje kunne vært unngått blant annet med politikernes

⁴ Terrorhandlinger reguleres i den nye straffeloven § 132

vilje. Politikk er et handlingssystem hvor det tas beslutninger innen økonomiske prioriteringer og lovgivning. Beslutningene angår samfunnet, dermed må retten og politikken forstås ut i fra det samfunnet det inngår i (Bernt og Doublet, 1999: 393). Luhman sin teori er i fra tidlig på 1990-tallet, en tid hvor man begynte å se fremveksten av teknologien for alvor, likevel var ikke teknologiens påvirkning på samfunnet i nærheten av hva den er i dag. Luhman forstod retten og politikken i lys av datidens samfunn samtidig som han nesten var forut for sin tid når han snakket om avhengighet av teknologiske løsninger. I dag er vi i den situasjon at vi er så avhengig av straffesakssystemenes funksjonalitet at de setter en stopper for ny straffelov. Kanskje kan man si at i det moderne, teknologiske, samfunn er vi avhengige av at teknologien fungerer tilfredsstillende fordi det er maskinene som styrer. Juristen er ikke enig i dette og mener at hvis politiet virkelig ønsket at loven skulle tre i kraft, hadde de klart å finne løsninger for det. Om ikke annet så på papir, istedenfor datasystemer.

Når det gjelder den nye straffeloven, har risikoen slått ut, det er ikke noe som kan skje, det skjer. Det er mangler ved systemene som har ført til at loven ikke trer i kraft. Dermed skiller risikoen seg ut på dette området i motsetning til de andre områdene hvor det foreligger risiko. På de andre områdene kan risikoen bli reell før eller siden eller så blir den reell av og til.

I nye systemer må det være enkelt å gjøre tekniske endringer slik at systemet kan utvikles i takt med tiden og rettsutviklingen. Det må være mulig å legge inn nye funksjoner og systemet må blant annet kunne håndtere endringer i lovverk, straffeprosess og statistikk.

4.5 Effektiv oppgaveløsning?

Straffesakseksperten forklarte alvoret ved risikoen med en humoristisk undertone: «Det med risiko knytter seg jo til et viktig samfunnsområde som er lov og orden og at vi ikke får beskyttet samfunnet mot kriminalitet. Isteden så sitter politiet å venter på å kunne starte PC-en igjen.»

Janet Chan skriver at teknologien alltid har påvirket politiet på en eller annen måte. Biler, radio, telefoner og datamaskiner har gjort det mulig for politiet å effektivisere sitt arbeid. Chan trekker frem at teknologi kan skape økonomisk gevinst ettersom effektiviteten økes uten at det trengs mer personale (Chan, 2003: 655). Det sier seg selv at utviklingen av teknologi vil

fortsette, og det i et hurtig tempo. Politiet må være forberedt på å stadig ta imot ny teknologi og nye systemløsninger. Teknologien er til hjelp samtidig som den bærer med seg noen utfordringer. I Politianalysen (2013: 200) står det at dagens systemer er foreldet og svært lite brukervennlige. Systemene jobber imot krav som effektivitet og kvalitet. Straffesakseksperten var opptatt av å fremheve at straffesakssystemenes lave brukervennlighet gir risiko for unødvendig tids- og ressursbruk. Det skaper et ineffektivt og utilgjengelig politi. Et av funnene i Riksrevisjonen undersøkelse av ikt-forvaltningen i straffesakskjeden (2012: 9) viser at ved å endre deler av IKT-systemene til politiet, kan det antas et gevinstpotensial på 280 til 460 årsverk. Funnet sier noe om hvor gammeldagse og tungvinte dagens systemer er. Straffesakseksperten bekrefter at MERVERDIprogrammet har kommet til tilsvarende tall i sine beregninger, og mener at da har de vært beskjedne.

Noe av det som skaper ineffektivitet er det faktum at systemene ikke snakker sammen. BL og Strasak kommuniserer ved at informasjon automatisk sendes fra BL til Strasak, men ellers er det ikke kommunikasjon mellom straffesakssystemene. BL kommuniserer derimot en begrenset mengde informasjon med et datasystem i domstolene, Folkehelseinstituttet og politiets etterlysningsregister. Det betyr det at kvaliteten i BL får følger i andre systemer enn bare BL og Strasak. Det finnes andre systemer, som for eksempel PAL, Indicia og agent, som henter informasjon fra straffesakssystemene, men det er kun uttrekk. For å få fullstendig informasjon opplæres brukerne til søkes direkte i kilden, altså i det aktuelle straffesakssystemet (Kriminalitetsbekjempelse og personvern). At straffesakssystemene ikke kommuniserer med hverandre utgjør en risiko fordi informasjonen i ulike systemer ikke nødvendigvis samsvarer. Samme informasjon må registreres i flere systemer for å skape helhet og sammenheng som systemene ikke finner automatisk. Straffesakseksperten sa:

Det er åpenbart at når vi ikke kan knytte sammen flere informasjonselementer så kan vi ikke identifisere overfallsmenn. Det går ofte bra, men vi kan ha problemer. Det går utenfor vanlig risiko. Vi kunne forhindre overfall, det er det lite fokus på. Sannsynligheten for det er umulig å beregne men når vi ikke kan sette sammen informasjon så har vi et problem.

Endres personinformasjon, for eksempel i SSP, blir ikke samme endring automatisk utført i de andre systemene. Informantene fortalte at mange brukere ikke vet hvor de kan finne relevant informasjon. Politiet har mange systemer som sier noe om de samme tingene, men få av systemene snakker sammen. Ikke alle skjønner konsekvensene av å ikke gjøre endringer i

flere systemer. Endres personidentitet bare i ett system blir det stående feil i alle andre systemer og det fremkommer ikke at det er samme person. Konsekvensen kan f.eks. bli mangelfulle straffeattester. I SSP registreres all informasjon på en *person*, mens i BL registreres alle opplysninger på en *sak*. Derfor er alt samlet i SSP, mens det er mer spredt i BL og Strasak. En personregistrering i SSP kan ha mange alias direkte knyttet til seg. Det kan derimot ikke registreres flere navn på samme person i BL, Strasak og BOT. Derfor kan samme personen være registrert en gang for hvert navn han eller hun operer med uten at det fremkommer at dette er samme person. Systemspesialisten fortalte om problematikken:

Det er et problem at du kan legge inn samme person flere ganger i personbasen i BL. Hvis du søker på en person, kan han ligge en gang med fullt fødselsnummer og 20 ganger i tillegg med bare fødselsdato. Det er mulig å slå disse sammen, det kan brukerne gjøre selv, men har en person flere identiteter, vet vi ikke om det er riktig å slå de sammen; at det virkelig er samme person.

Brukeren fortalte om det samme:

En person registreres på nytt i BL hver gang han får en ny sak. Det er rutine å hekte det sammen så alt synes på samme person, men hvis man da blander dag og måned og registrer på noe annet enn sist, så blir det ikke koblet sammen. Det er jo et pes å endre i etterkant, skal man endre og hvem skal endre? Jeg savner mer kontroll på det. Det må kanskje lages nye rutiner, men det kommer vel etter hvert.

Det er kun i SSP at det er mulig å generere unike fiktive numre for de som ikke har norsk personnummer. Dermed kan det være vanskelig å se om det er samme person som er omtalt i de ulike systemene eller ikke. Det kan også risikeres at ikke alle sakene kobles til den samme personen i de andre systemene. Brukeren fortalte også at det ikke er noen rutiner for å endre registrert identitet på en person i BL når saken er avgjort. Selv om det oppdages at en person er registrert med feil personopplysninger, blir det opp til den enkelte bruker om det skal rettes opp i eller ikke. Det betyr at historikken kan bli liggende med feil informasjon for alltid.

Alle informantene er enige om at det er svært tungvint å bruke systemene fordi det må søkes og registreres både i SSP, Strasak, BL og BOT for å få et helhetlig bilde. Gundhus fant det samme i sin undersøkelse. Hun skriver at enkelte velger å ikke registrere informasjon fordi registrering oppfattes som teknisk vanskelig og tungvint (Gundhus, 2006: 228). Gundhus viser også til en undersøkelse hvor det kom fram at det er 105 ulike elektroniske systemer som kan være nyttige i politietterforskning. Av politiregistre som brukes som informasjonskilde i hverdagen er det ca. fire (Gundhus, 2006: 58). Noe av den største utfordringen for politiet når det gjelder IKT er at det er store mengder informasjon tilgjengelig

i de ulike systemene. Det blir vanskelig for brukeren å finne det som er nødvendig, og skille det ut fra det som er overflødig informasjon (Gundhus, 2006: 61) Et utdrag fra et av intervjuene belyser problemet med at det må søkes i mange systemer når det skal avgjøres om informasjon skal slettes fra systemene eller ikke. Når en sak henlegges, er det informasjon som må slettes, men det kan finnes andre saker som gjør at informasjonen likevel kan beholdes. Å finne ut av dette for å fatte korrekt avgjørelse er ikke alltid like enkelt:

X: jeg jobber jo ikke så mye med det i praksis, men selv så lite som jeg jobber med det så er det jo til å bli gæren av. Det er jo så tungrodd, mye tasting. Samme informasjon må inn i forskjellige systemer. Nå må jeg i flere systemer for å se etter samme informasjonen, og noen ganger vegrer jeg meg. Jeg må i alle fall søke samme tallrekke i tre systemer.

Meg: Hva skjer hvis du glemmer et system?

X: Jeg glemmer det ikke for da mangler jeg en del av bildet, men noen ganger gidder jeg ikke. Noen ganger ser jeg at en person skulle vært slettet, men jeg orker ikke søke mer og jobbe mer for å finne den informasjonen jeg trenger. Nå lager PDMT slettelister. Hvis noen ikke har pågående saker får vi beskjed om at de skal slettes. Sånn var det ikke for inntil et par år siden. Det kan bli et rettssikkerhetsproblem når noen ligger i systemene lenger enn de skal.

PDMT lager altså slettelister for noen systemer slik at man automatisk finner opplysninger og personinformasjon som skal slettes. Andre systemer har ikke tilsvarende funksjoner, og er derfor avhengig av manuell kontroll. Det er i de tilfeller denne kontrollen svikter at opplysninger som skulle vært slettet ikke blir det. I slike tilfeller er det den siktede sin rettssikkerhet som eventuelt svekkes fordi staten beholder opplysninger om borgeren utover den tiden de har lov til. Det er ikke dermed sagt at opplysningene brukes, og de slettes når det oppdages at det ikke lenger er hjemmel for å beholde dem. Juristen trekker frem behovet for å ta vare på opplysninger. I politiregisterloven er det regler for hvilke opplysninger som må slettes og når de må det. Slettingen kan true rettssikkerheten ifølge juristen, som trekker frem et eksempel:

Man kan også si at det er et rettssikkerhetsproblem at man ikke får lov til å ta vare på de opplysninger man trenger. Hvis jeg blir ranet på åpen gate så oppfatter jeg det som et rettssikkerhetsproblem hvis opplysninger i den saken må slettes, men det er nok ikke det man tenker på som et generelt rettssikkerhetsproblem.

I sitatet er rettssikkerheten altså knyttet til sletting av opplysninger. Juristen ser for seg at slettingen gjør at politiet har mindre informasjon og dermed ikke får tatt raneren. Rettssikkerheten, i sin klassiske betydning jf. Robberstad (1999: 360), svekkes altså. Ettersom juristen avslutter med å si at det ikke er det man tenker på som et generelt rettssikkerhetsproblem, kan det tyde på at juristen har en nyere forståelse av begrepet enn den

klassiske. Videre sa juristen at det kan virke som om politiet gjør ting de ikke har lov til fordi de diskuterer problemstillinger rundt lovverket høyløst, men det at de tar diskusjonen betyr ikke at de gjør noe galt i praksis:

Meg: Er politiet flinke til å ivareta kravene til personvern i sin bruk av teknologiske løsninger?

X: Det kommer nok an på hvem du spør. Det er et annet fokus på det nå enn for bare litt siden. Jeg synes etaten er ryddig og ordentlig, men det går på tvers av det å skulle fange kjeltringer. Man registrerer ikke mer enn man får lov til, men man krangler om å få lov til å registrere mer. Så etaten gjør det de skal, men de tar diskusjonen likevel. Noen mener at personvern har fått for stor plass.

Meg: Hender det at ulike behov går på bekostning av hverandre?

X: Politiet tar ikke vare på opplysninger man ikke skalt ta vare på, men vi sier tydelig fra når vi mener noe er feil. Eksempel er pass eller datalagringsdirektivet. Man får kanskje inntrykk av det motsatte fordi det er så mange høyløste diskusjoner. For meg kan personvern like gjerne være mer registrering enn mindre registrering, for å få bedre kvalitet.

Juristen sa altså: «Jeg synes etaten er ryddig og ordentlig, men det går på tvers av det å skulle fange kjeltringer.» Ut ifra resten av sitatet tolker jeg juristens utsagn til at politiets lovløshet gjør at de ikke får stoppet like mye kriminalitet som de kunne gjort om de hadde brutt regelverket og tatt vare på flere opplysninger enn de har lov til.

Juristen fortalte også om SSP og sa at det er bemerkelsesverdig hvor mange personer som registrerer, hvor mye tid det tar og hvor overraskende lite informasjon politiet sitter igjen med. Informanten mener at i 2013 bør det kunne forventes å få mer utfyllende informasjon enn det SSP gir. I SSP er det, som jeg så vidt nevnte i kapittel 4.2, begrenset plass for fritekst. Det betyr at tekst som legges inn må forkortes. Informasjon som legges inn som fritekst er informasjon det ikke finnes koder for. Noe av informasjonen kan finnes i andre systemer slik at det er mulig å finne ut av betydningen hvis den er uklar.

Det er mange utfordringer som skapes fordi systemene ikke kommuniserer bedre med hverandre. Informantene fortalte om mulige konsekvenser som kan gå ut over enkeltpersoner som er registrert i systemene.

Meg: Snakker de ulike systemene med hverandre eller med noen andre systemer?

X: Ja, det var det da. Det er fint lite, de snakker ikke sammen. Det er jo BL/Strasak da, men de hører jo sammen. Noen av de nye systemene, med signalement og sånt, snakker vel sammen, men det kan ikke jeg så mye om.

Meg: Hvilke konsekvenser har det at systemene ikke snakker sammen?

X: Ja, det er utrolig mye. Folk blir tatt inn med et navn og det blir registrert i saken. Så blir han domfelt og avgjort sak i det navnet. Etterpå skjønner man at det kanskje ikke var rett og at det kanskje er mer informasjon på samme person, men registrert med annen id.

Meg: Hvilke konsekvenser kan det, i verste fall, få?

X: Det blir jo feil i politiets registre for alltid.

Meg: Kan det skje at en person blir registrert med en id som tilhører en annen?

X: Ja, det kan det. Og historikken på hva personen har gjort blir feil. Straffemessig kan det jo skje at personen får lavere straff enn han skulle hatt. Får kanskje et forelegg når han egentlig skulle hatt dom. I verste fall kan jo feil person ta straffen.

En og samme person kan registreres med ulik personinformasjon slik at det ser ut som om det er flere personer. Saksopplysninger og reaksjoner kan også bli registrert på feil person, kanskje en som er helt uskyldig. Dette fører igjen til mangelfulle straffeattester og historikk. Hvis en person er registrert flere ganger på ulike identiteter ser det ut som om personen har gjort færre straffbare ting enn det som ville fremkommet om alle sakene var registrert på samme identitet. Hvis feilen ikke oppdages kan det føre til at en dommer gir straff ut i fra mangelfulle opplysninger, og straffen vil da bli lavere enn om alle forholdene var kjent. Dermed beskyttes ikke borgerne mot overgrep fra den siktede i like stor grad som de ville blitt om alle forholdene var kjent og straffen kunne vært skjerpet. Som oftest er det færre saker registrert på den skyldige enn det som er riktig. I omvendte tilfeller vil den skyldige raskt protestere og feilen rettes. For den skyldige oppleves det som en fordel å få for lav straff, men for resten av samfunnet betyr det at de ikke beskyttes mot lovbrøtteren slik de har krav på. Informantene vet ikke noe om omfanget av dette. Brukeren mener at slike tilfeller oppdages relativt raskt og rettes opp i. Juristen fortalte:

Meg: Er informasjonen som ligger i systemene fullstendig og korrekte?

X: Ja, det tror jeg. Med unntak av identitetsproblematikken. Man vet ikke hvem folk er. Man tror man snakker med en, men så er det fetteren. Det ligger derfor reaksjoner på feil personer og fingeravtrykk med feil personinformasjon.

Meg: Hvilke konsekvenser kan det få?

X: At rettferdigheten ikke skjer fyldest og det går på rettssikkerheten løs. Feil personer kan få reaksjoner de ikke skulle hatt, men det kan også være overlatt. Noen betaler andre for at de skal sone for seg. Andre ligger i systemene våre uten at det aner det. Det skulle vært morsomt å vite hvor mange slike tilfeller det er. Hvis det er tatt fingeravtrykk kan det jo oppklares, men uten er det trøbbel.

Det er her snakk om en identitetsproblematikk som kan få alvorlige konsekvenser, men jeg ønsker å presisere at dette ikke bare handler om straffesakssystemene. For eksempel spiller også opptak av biometri inn, men det ligger utenfor mitt undersøkelsesfelt. Jeg spurte likevel juristen om hvordan man kan løse utfordringen med registrering av personer med ukjent identitet: «Jeg er ikke sikker. Det er best å registrere alle saker, til slutt vil man finne ut av det. For ofre er det også best at alt er registrert. Jo mer informasjon, jo lettere er det å finne sannheten, men man må ha tillit til myndighetene.» Tilliten kommer jeg tilbake til i kapittel 5.

Identitetsproblematikken gjør det vanskelig for politi og påtalemyndighet å gjøre jobben sin, og det går mye tid på å rette opp slike registreringsfeil. Brukeren fortalte at de registrerte kan rammes, av de grunner som er nevnt over, når brukerne har gjort feil ved registrering eller søking etter informasjon. Grunnen til at brukerne gjør feil er ofte at systemene er tungvinte å søke i, ikke snakker sammen, har ulikt kodeverk og har forkortet informasjon som gjør at det er vanskelig å forstå hva som står. Feilene som skyldes menneskelige registreringsfeil, og ikke svikt i straffesakssystemene, kunne altså vært unngått om systemene var bedre tilrettelagt slik at det ble lettere å registrere riktig. Systemspecialisten sa at det er menneskelig å gjøre feil innimellom, men «Vi må stole på at folk kjenner sine arbeidsoppgaver og vet hvordan verktøyet skal brukes». Ifølge systemspecialisten er det først og fremst brukerne som rammes av de tekniske feilene i systemene fordi de må bruke lenger tid på arbeidsoppgavene sine. Straffesakseksperten tror at tidsbruken kunne kommet publikum til gode. Informanten fortalte:

Et område som lider hele tiden det er forbyggende. Å forhindre nye straffbare forhold. Vi har kunnskap om metodikk og kriminalitet og vi kan lage problemanalyser, men min påstand er at vi kunne forminsket kriminalitet, hadde vi visst det vi vet. Jeg har en hypotese om at 20 % av kriminaliteten kan fjernes. Det er en etisk problematikk; vi vet hvordan, men vi får ikke gjort det fordi vi har dårlig tilgang på informasjon.

Det blir ren gjetting å anslå hvor stor effekt nye systemer vil ha på oppklaringsprosenten, men straffesakseksperten har et poeng. Hadde politiet kunne bruke arbeidstiden på kjerneoppgavene sine, kunne kriminalitet vært unngått. Riksadvokat Tor-Aksel Busch, sier noe av det samme: «Bedre IKT-støtte frigjør tid og ressurser som kan brukes til å behandle saker raskere, og til å etterforske saker som i dag må henlegges av kapasitetsgrunner.» (MERVERDIprogrammet informasjonshefte 2013-2014). Alle informantene sa at det kan bli for mye informasjon hvis det kan søkes i all informasjon politiet har. Tilgangsnivåene må derfor begrenses slik at den enkelte bruker har tilgang til rett informasjon i henhold til rolle og oppgaver.

I diskurser om politiarbeid er det ofte snakk om det operative arbeidet, og det omtales gjerne som et spenningsfylt og til tider farlig yrke. Chan viser at noe av grunnsteinen i politiarbeidet er informasjonsinnhenting (Chan, 2003: 657). Et kunnskapsbasert politi er helt avhengig av gode datasystemer. Når informasjon er samlet inn gjør datasystemene det mulig å dele, sortere

og analysere informasjonen (Chan, 2003: 658). Tilgangen til all informasjonen kan bli oppfattet som rotete av brukerne ved at man ikke finner det man leter, etter eller ikke klarer å sortere ut det som er relevant. Chan viser til flere studier som har vist at selv om IKT-verktøy bidrar til økt produktivitet, henger ikke nødvendigvis effektiviteten med (Chan, 2003: 661). Det er mulig å se for seg at mindre tid på PC-en kan brukes til forebygging av kriminalitet og oppklaring av lovbrudd, men denne påstanden er vanskelig å måle. Hvis det er en realitet betyr det at borgerne kunne vært beskyttet mot hverandre i sterkere grad enn de blir med dagens straffesakssystemer.

Ericson og Haggerty (1997) ser politiet som kunnskapsarbeidere. De viser til mangfoldige undersøkelser som sier at politiet bruker lite tid direkte på kriminalitet. Mesteparten av det daglige arbeidet handler om å finne og kontrollere risikoer, og det innebærer mye papirarbeid. Likevel er det ordentlige politiarbeidet ofte forbundet med arbeid direkte knyttet mot kriminalitet (Ericson og Haggerty, 1997: 19-21). Politianalysen har valgt å definere politiets kjerneoppgaver til å gjelde opprettholdelse av alminnelig orden, forebygging av straffbare handlinger og beskyttelse av borgerne og deres lovlige virksomhet (Politianalysen, 2013: 77). Finstad skriver at det *egentlige* arbeidet er det som oppfattes som kjernen i et yrke. For politiet er det en utbredt oppfatning at kjernen er å fange røvere (Finstad, 2013: 98-99). Papirarbeid kan forstås som en del av det egentlige politiarbeidet selv om det ikke er det man tenker på som en kjerneoppgave. For å fange røvere må kunnskap om dem tilegnes. Det kan gjøres gjennom rapportskrivning, informasjonsinnhenting og analyser. Kunnskapspolitiet kjennetegnes av store mengder papirarbeid, enten papir i sin opprinnelige form eller elektronisk. Ericson og Haggerty hevder at mellom 30-80 prosent av arbeidstiden til polititjenestepersoner går til papirarbeid avhengig av hva slags politi vedkommende er, eksempelvis trafikk, orden eller forebyggende (Ericson og Haggerty, 1997: 296). Hvis papirarbeidet stadig forstyrres av tekniske feil og lav brukervennlighet, kan straffesakseksperten ha rett i at tidsbruken kunne kommet samfunnet bedre til gode dersom tiden ble bedre utnyttet. I stedet for å bruke tid på tekniske feil kunne politiet brukt tiden til papirarbeid. Undersøkelsene som Ericson og Haggerty utførte viste at politiet selv mener det ordentlige politiarbeidet er å være ute i gata. Samtidig innså politiet at mesteparten av kriminaliteten ikke kunne forhindres uten å utføre kunnskapsarbeid, papirarbeid og risikoanalyser. På tross av at politiet så koblingen mellom papirarbeid og forebygging, mente

de likevel at feltarbeid var det ordentlige politiarbeidet (Ericson og Haggerty, 1997: 299). Papirarbeid er altså det som gjør politiet kunnskapsbasert, og det er politiet selv som ønsker og trenger kunnskapen de bruker mesteparten av tiden sin på å finne (Ericson og Haggerty, 1997: 21).

Gundhus har rangert ulike kunnskapstyper ved en politiavdeling hun har kartlagt. Rangeringen viser at analyse, statistikk, registeropplysninger og teoretisk kunnskap har lav status og blir sett på som standardiserte opplysninger. Av høyere rang er erfaringsbasert kunnskap som fersk informasjon, konkret og individuell kunnskap, levende informasjon fra informanter og erfaring som magefølelse og intuisjon (Gundhus, 2006: 117). Samtidig skriver hun at flere av informantene hennes hevder at registerkontroll og identitetssjekk er det viktigste kunnskapsarbeidet. Søk i registre er også den vanligste måten å bruke IKT på (Gundhus, 2006: 207). Gundhus skriver at det er delte oppfatninger om hvorvidt IKT i politiet er en trussel eller noe som skaper muligheter. De som ser det som en trussel gjør det fordi det stadig er tekniske problemer (Gundhus, 2006: 90). Det kan også virke begrensende i forbindelse med administrasjon og rutine- og papirarbeid (Gundhus, 2006: 209). Det er rutinearbeid å legge inn informasjon i registrene. Dermed er det viktigste kunnskapsarbeidet avhengig av at det er gjort en god jobb ved rutinearbeidet som preges av begrensninger fra straffesakssystemene.

Chan (2001) sin undersøkelse fra Australia på slutten av 90-tallet, viste at de fleste politifolkene mente deres arbeid hadde blitt effektivisert etter innføringen av etatens datasystemer. De aller fleste mente også at det hadde blitt lettere å drive informasjonsdeling, lettere å samarbeide og at effektiviseringen var positivt for arbeidsmiljøet (Chan, 2001: 149). Den samme undersøkelsen viste at innføringen av IKT var grunnen til at politiet brukte mer tid på papirarbeid som analysering og planlegging (Chan, 2001: 150). Dette kan være fordi de opplevde at mer tid med papirarbeid bidro til mer effektiv oppgaveløsning. Det forutsetter at systemene fungerer som gode verktøy, og at det ikke stadig er tekniske feil og driftsavbrudd. På den andre siden viste undersøkelsen at noen ting gikk saktere enn før. Rapporter som skulle fylles ut hadde flere rutinetripp enn tidligere, og det tok derfor mer tid. Noen mente at de nye rutinetrippene ikke var en følge av IKT-innføringen, men et resultat av lovgivning og regelverk (Chan, 2001: 152).

Ericson og Haggerty sier at politiarbeid ikke er ad hoc og handlingspreget, men strukturert etter risikovurderinger og IKT (Ericson og Haggerty, 1997: 33). Det kan diskuteres om det er dekkende for reell praksis ettersom operativt politiarbeid ofte omtales som både ad hoc og handlingspreget. «The police are knowledge workers who join other major institutions in believing that the world can be made more secure by ever more perfect knowledge of risk» (Ericson og Haggerty, 1997: 295). Etter mine funn, som viser at politiet ikke har systematiske risikoanalyser av straffesakssystemene, kan det synes at det norske politiet ikke lever helt opp til dette sitatet. Eller så er risikokunnskapen mer rettet mot lovbrøyttere og avviksgruppene i samfunnet, enn innad på politiet selv. Et tredje alternativ er at det finnes systematiske risikovurderinger, men at disse er taushetsbelagt og at jeg derfor ikke har fått noe informasjon om disse gjennom mine intervjuer. Sistnevnte alternativ innebærer at mine informanter ikke visste om disse risikovurderingene eller at de løy da de fortalte at det ikke fantes. At de ikke visste om det virker usannsynlig med tanke på posisjonen særlig til straffesakseksperten og systemspecialisten. Jeg fikk heller ikke følelsen av at informantene holdt tilbake informasjon eller løy.

Videre sier Ericson og Haggerty at den perfekte kunnskapen om risiko aldri kan nås fordi mer kunnskap avdekker mer risiko. Å prøve å oppnå perfekt mengde kunnskapen blir en evig sirkel (Ericson og Haggerty, 1997: 296). «Although police officers know they cannot live without their knowledge systems, they constantly find it difficult to live with them» (Ericson og Haggerty, 1997: 301). Kanskje har norsk politi forsonet seg med at straffesakssystemene er utdaterte og må fornyes. Risikoanalyser vil være bortkastet tidsbruk fordi mer kunnskap vil avdekke mer risiko. Ericson og Haggerty mener at innføring av mer teknologi ikke har ført til effektivisering eller færre ansatte fordi kunnskapsbehovet aldri slukker og ny teknologi kommer med nye krav (Ericson og Haggerty, 1997: 301). I lys av dette, kan man lure på om nye straffesakssystemer ikke vil virke effektiviserende. Sannsynligvis vil risikoelementene som foreligger i dagens systemer minke, hvis ikke ville det ikke være noen vits å lage systemene. Men kanskje kommer det nye eller andre typer risikoer som ikke er forutsett. Kanskje vil systemene bidra til effektivisering på enkelte områder, mens andre områder forblir som i dag. Brukeren fortalte om en ekstrem stor arbeidsmengde og tidspress som gjør at det slurves med kvalitetssikring, kontroll og registreringer. Nye systemer må være enklere og bedre tilrettelagt for brukerne slik at det kan bli kortere tidsforløp i saksbehandlingen. For å få til dette må det være færre rutinetripp, lettere å registrere, bedre søkemuligheter og samlet

personinformasjon. Samlet personinformasjon vil også gjøre det enklere å ivareta kontroll av identitet.

4.6 Kunnskapsdeling

Lite opplæring og lav systemkunnskap utgjør en risiko fordi politiet ikke vet det politiet vet.

Selv om informasjon er registrert, kan det være vanskelig å finne frem til informasjonen.

Brukeren mente at lite opplæring er en gjenganger ved alle straffesakssystemene:

Meg: I hvilken grad tilbys det opplæring i SSP, BOT, BL og Strasak? Hvordan foregår opplæringen?

X: Nei, den er vel fint lite. Sånn lesemessig, som juristene og etterforskerne, bruker SSP bare til å lese. Vi som registrerer inn får ymse opplæring. Før var det superbrukere og fast opplæring. Fra Kripas sin side er det fortsatt strengt, men det er ikke så strengt i distriktene.

Meg: Er det fordi SSP ikke blir sett på som så nøye?

X: Ja, jeg tror det. Det har forandret seg til det bedre de siste to årene, men det handler om å finne de rette personene. Jeg tror ikke det har vært noen helhet.

Meg: Er det mer konkret opplæring i BL med tanke på de oppgavene man har?

X: Det er jo opplæring, men learning by doing. Det kan gå lang tid før man oppdager noe lurt og smarte funksjoner. Ellers får du opplæring på akkurat den oppgaven du har. Juristene får eget BL kurs, men de jobber mye med det. Påtalemodulen i BL er stor.

Meg: Tror du potensiale i systemene er større enn folk tror fordi folk ikke har nok opplæring og kunnskap?

X: Ja, det tror jeg. Absolutt. Særlig etter at det kommer flere og flere utlendinger⁵. Men jeg tror ikke folk vet at det er et større potensiale der.

Studentene på Politihøgskolen har et eget emne som heter Digitalt politiarbeid. Gjennom dette emnet skal studentene tilegne seg kunnskap om og lære å benytte sentrale datasystemer.

Denne opplæringen skal også være en del av praksisåret (Politihøgskolen.no). Brukeren

fortalte at opplæringen av sivilt ansatte gjerne går på en konkret oppgave, som for eksempel registrering av forelegg i SSP, men at det blir lagt lite vekt på helhetsforståelsen for systemet.

Brukerne må selv finne frem til ulike funksjoner eller informasjon som kan være tilgjengelig.

Juristen sa at det sannsynligvis er mer informasjon i registrene enn det den vanlige politimann forstår fordi informasjonen er så komprimert. Videre sa juristen: «Du må være født og

⁵ Her mener informanten at det registreres stadig flere utlendinger i systemene. Registrering av personer uten norsk personnummer er komplisert fordi systemene krever et personnummer, og fordi det er vanskelig å vite hvem vedkommende er. Registrering av personer uten norsk personnummer krever opplæring og kunnskap slik at systemenes fulle potensiale kan utnyttes.

oppvokst på Kripos for å forstå hva som står i systemene. Det er nok en grunn for at man registrerer slik man gjør selv om de nok ikke lever lenger de som vet grunnen til det.» Med dette mener juristen at det er de som var med å bygge opp systemene som vet hvorfor det registreres slik det gjør, og at denne kunnskapen i liten grad har vært dokumentert for etterkommerne. Sitatet belyser, nok en gang, at politiet arbeider erfaringsbasert. I kapittel 4.2 skrev jeg om PDMT som har et fåtall av personer som innehar kunnskap om stormaskinen til Strasak, hvor avhengig politiet er av disse personene og at de snart pensjoneres. Det vitner om at kunnskapen er lite dokumentert og at politiet er for dårlig på kunnskapsdeling. Dette ble påpekt i Accenture-rapporten (2010: 19) hvor det står at sentrale kompetanseområder er underbemannet, og at det er vanskelig å finne tid til opplæring. Videre står det at det er planer som skal ta hånd om dette. Likevel fortalte min informant om det samme problemet tre år etter at rapporten ble utgitt. Rapporten fastslår at kunnskapsdeling ikke er tilstrekkelig innarbeidet i PDMT og dette reduserer effektiviteten i organisasjonen (Accenture-rapport, 2010: 40).

En institusjonell hukommelse, som for eksempel rutinebeskrivelser, vil bidra til mer kollektiv kunnskap som kan minke risikoen for lite opplæring, lav brukervennlighet og ulike registreringsmetoder. Brukeren fortalte at bevisstheten rundt en institusjonell hukommelse har bedret seg de siste årene. Videre sa informanten at SSP er et system som brukes annerledes av ansatte på Kripos enn i distriktene. I distriktene bruker de det mindre, de er mindre nøye med kvalitetssikring ved registrering, og brukerne skjønner hverken potensialet til systemet eller det som står der. Et sitat fra intervjuet med brukeren beskriver mangelen på kunnskap om viktigheten av registrering i systemene:

...mange tenker nok at det ikke gjør noe om det er feil fordi det er ingen som kontrollerer eller bruker informasjonen uansett. Jeg vet jo ikke det men ... Det var en som foreslo at vi skulle kaste alle arrestjournalene, uten å registrere dem, så de ser jo ikke nytten av SSP. Kvalitet står nok ikke så høyt i kurs hos alle.

En arrestjournal er en rapport som forteller hvem som er pågrepet, for hva, gjerningssted og gjerningstid. Å la være å registrere en arrestjournal i SSP er imot regelverket og relevant historikk blir ikke dokumentert. Å registrere arrestjournaler gir politiet informasjon, å la være vil bety at informasjonen ikke deles. Det er forståelig at brukerne blir frustrerte over at de må registrerer de samme opplysningene i flere systemer, i dette tilfelle både i BL og i SSP. Så lenge straffesakssystemene ikke snakker sammen, er det helt nødvendig. Brukeren fortalte at

den store arbeidsmengden gjør at det fort blir restanser. Dermed er det ikke oppdatert informasjon i systemene.

Gjennom intervjuene fikk jeg en forståelse av at SSP er en «Kriposgreie». Alle fire informantene sa at det er Kripos som styrer og bruker SSP. Det er bemerkelsesverdig at det bare er Kripos som ser hvor sentralt SSP er og hvilken tyngde informasjonen der har. SSP inngår heller ikke i rådet for elektronisk straffesaksbehandling (RESP) selv om systemet er en del av den elektroniske straffesaksbehandlingen. Straffesakseksperten fortalte at Kripos tar seg av SSP, derfor er ikke systemet en del av RESP. Support på SSP er heller ikke en del av straffesaksteamet ved PDMT. Dette er tydelige eksempler på at politiet sitter på hver sin tue og at det er en vei å gå når det gjelder opplæring.

Brukervennlighet og opplæring er, ifølge Northrop mfl. (1995: 268-269), de to viktigste faktorene for at datasystemene kan fungere som effektive hjelpemidler for kriminalitetsbekjempelse. Northrop mfl. (1995: 271) skriver også at mange velger å ta seg tid til å lære seg datasystemene fordi de ser nytten av det. Forfatterne har et viktig poeng: «Only through adequate training can police users of search systems begin to understand the vital link they play as both consumers of information from the systems and suppliers of information to the systems» (Northrop mfl., 1995: 272). Videre skriver de at det ikke hjelper å bruke mye penger på moderne systemer hvis ikke det legges ned tid og ressurser til opplæring. I undersøkelsen til Northrop mfl. viste det seg at datasystemene bidro til oppklaringen av over halvparten av de oppklarte sakene, uavhengig av type sak (Northrop mfl., 1995: 264). Det er viktig å ikke glemme dette; hvor relevante systemene er i motsetning til å ikke ha noe datateknologi. Selv om en kunne forvente mer av politiets systemer enn det som kommer ut av dagens straffesakssystemer, er det bedre enn å ikke ha noe. Studien deres viser også at de færreste får den opplæringen som er nødvendig, og ofte går opplæring og brukervennlighet på bekostning av hverandre. Har systemet høy brukervennlighet, blir det lite opplæring, men hvis systemet er lite brukervennlig, blir det mer opplæring. Northrop mfl. (1995: 270) mener at det bør være opplæring uavhengig av hvor god brukervennligheten er.

Både brukeren, systemspecialisten og juristen fremhever at vi kunne gjort mer med det som finnes av systemer i dag. Politiet vet ikke det politiet vet fordi systemene ikke er gode nok. Dette ble påpekt blant annet i lommemannsaken. Lommemannsaken var en omfattende

overgrepssak hvor det tok relativt lang tid før sammenhengen mellom de ulike overgrepene ble oppdaget. Dermed tok det også lang tid før saken ble oppklart og overgriperen pågrepet. I en artikkel i Aftenposten fra 2009 står det at politiet tar lærdom av lommemannsaken. Et utvalg som gikk gjennom etterforskningen av saken kom med 27 forbedringspotensialer for politiet. Et av dem lyder: «Dataverktøyet politiet bruker inneholder mye informasjon, men er dårlig egnet til effektiv etterforskning» (Aftenposten, 2009). Ifølge juristen siktes det her blant annet til BL og Strasak, informanten fortalte:

Det er noe med hva man registrerer også. Hadde noen skrevet *drops i lomma*, så kanskje man hadde koblet det før. *Forsøk på seksuell kontakt* blir for generelt. Det var der det sviktet, man registrerte ikke alt. Kritikken i lommemannsaken var altså at man ikke registrerte alt, og at det ikke var tilgjengelig på tvers. Det siste var systemenes skyld, det første var personsvikt.

Det er altså både systemene og en del menneskelige svikt som gjør at politiet ikke får utnyttet den informasjonen som finnes. Den menneskelige svikten går ofte på for dårlig opplæring og for lite kunnskap om systemene og registreringen, ifølge informantene.

4.7 Snokekultur

Pr. dags dato er det ikke teknisk mulig for straffesakssystemene å oppfylle alle kravene i politiregisterloven. Det utgjør en risiko fordi det kan skape en snokekultur. Juristen fortalte at den kommende politiregisterloven regulerer hva politiet skal og kan registrere. I tillegg inneholder loven bestemmelser om sletting, retting, tilgang, sporing og logging. Når det gjelder hva som kan registreres, blir det en videreføring av gjeldene rett. Juristen mener at det ikke er noen hull i dagens lovverk, men informanten savner at det åpnes for å ta vare på mer biometri for identifikasjonsformål. Hvis lovverket åpner for å ta vare på flere opplysninger kan politiet forebygge mer. Ellers sa juristen at det er positivt at slettereglene blir tydeligere i ny politiregisterlov enn de har vært tidligere.

Politiregisterlovens ikrafttredelse har blitt utsatt gang på gang fordi loven har blitt sett i sammenheng med datalagringsdirektivet. Utgangspunktet var at politiregisterloven skulle tre i kraft samtidig med datalagringsdirektivet for å ha et regelverk som håndterte ivaretatte

opplysninger på en god måte. Når datalagringsdirektivet ble utsatt, hastet det ikke for politiregisterloven heller, men i 2012 ble det bestemt at politiregisterloven skulle tre i kraft uavhengig av datalagringsdirektivet. Datoen for ikrafttredelsen av politiregisterloven og tilhørende forskrift er satt til 01.07.14. I dag oppfyller ikke straffesakssystemene politiregisterlovens krav til sporing og logging. Det betyr at det ikke er mulig å se hvem som har registrert hva. Problematikken er kjent. Når nye straffesakssystemer kommer, skal alle kravene i politiregisterloven tilfredsstilles, også kravene til sporing og logging. Dette betyr at det må bli bedre redigeringsmuligheter og mulighet for å se registrert historikk, altså hva som tidligere var registrert og i noen tilfeller informasjon om hvorfor det er endret. Slik logginformasjon kan for eksempel være viktig når personinformasjon endres etter å ha avdekket falsk identitet. Kravet til sporbarhet vil kunne avdekke urettmessig behandling av opplysninger.

I Accenture-rapporten (2010: 24) fastslås det at politiet har liten innsikt i fremtidige behov som utløses av nytt lovverk og forskrifter. Juristen fortalte at det har det vært nedlagt mye arbeid vedrørende det nye lovverket siden 2010. Det er derfor sannsynlig at behov som utløses i forbindelse med lovverket nå er bedre kjent enn det var da Accenture-rapporten ble utarbeidet for fire år siden. Juristen mener at dagens lovverk ikke er dårlig, men det er laget i en tid hvor det ikke fantes elektroniske systemer. Derfor er det behov for nytt lovverk. I dagens samfunn er det også et annet fokus på personvern enn det har vært tidligere, det må imøtekommes i politiets registre. Det nye blir at lovverket stiller krav til sporing og logging, og at man kan se hvem som har gjort hva i systemene. Poenget med dette er å bli kvitt snokekulturen, fortalte juristen. IKT har skapt nye politikulturer, ifølge Chan (2003: 661). Kanskje er snokekulturen et eksempel. Snokekulturen kan ha utsprunget tidligere, men tilgangen på store mengder informasjon gjør det lettere å snoke nå, enn det var i en papirmølle.

I en tidligere årsrapport skriver Spesialenheten for politisaker om politiets misbruk av registeropplysninger. Jeg har ikke funnet konkrete tall på dette, men Spesialenheten skriver at av de anmeldte sakene for brudd på taushetsplikten, er det ikke sjeldent at den mistenkte har søkt i registrene uten tjenestemessig grunn (Årsrapport 2010: 9). Spesialenheten presiserer at det er et ledelsesansvar at rutiner, instruksjoner, regler og retningslinjer er kjent og følges av ansatte i politiet. Samtidig etterspør spesialenheten at ledere faktisk tar dette ansvaret (Årsrapport 2013: 25). Spesialenheten for politisaker etterlyser derfor en mer engasjert og

tydelig ledelse for å forebygge straffbare handlinger begått av politiansatte (Årsrapport 2013: 24). Det er ikke lov å søke i politiets registre uten tjenestemessig grunn for søket. I årsrapporten for spesialenheten står det at politi som avhøres i denne typen saker forklarer at det er lokalt akseptert å søke etter informasjon selv om det ikke er til tjenesteformål (Årsrapport 2013: 25). I avvikshistorier som presenteres i media fremstilles ofte den skyldige som et råttent eple blant ellers friske (Reiner, 2003: 269). Med ny politiregisterlov og nye straffesakssystemer med loggfunksjoner blir risikoen trolig mindre, enn i dag, for at det oppstår snokekulturer. Politiregisterloven og nye straffesakssystemer kan bidra til at det blir færre råtne epler i politiet fordi det vil bli større sannsynlighet for å bli tatt.

Politiregisterloven stiller også krav til notoritet og tydelighet. Straffesakseksperten fortalte om behovet: «Vi trenger et system som fungerer, og vi trenger informasjonsflyt som vi ikke har i dag. Det å få kunnskap i forhold til den rollen du har som gjør at du kan løse den oppgaven du er satt til, det sparer tid og gir bedre notoritet.» Informasjonen i straffesakssystemene må derfor gå til brukere i alle roller, det være seg jurister, etterforskere eller saksbehandlere. All informasjon må være tilgjengelig i ett system, og så må heller tilgangene begrenses.

4.8 Situasjonen gir ingen fordeler for politiet

Flyghed og Hörnqvist (2003: 9) hevder at alt staten gjør i krigen mot terror, som tilsynelatende skjer for borgernes sikkerhet, ikke er positivt eller nødvendig. Staten skal forsvare lover, orden, rikets indre og ytre sikkerhet og det demokratiske styresettet, men forfatterne mener at staten overgår lover og skaper en lovløs tilstand hvor rettigheter fratras (Flyghed og Hörnqvist, 2003: 11). Forfatterne tar opp hvordan noe tilsynelatende er trygghetsskapende for borgerne, men likevel svekker andres rettssikkerhet. Dette bidraget har kanskje ikke selvsagte tråder til min oppgave, men jeg har valgt å ta det med fordi det belyser hvordan noe tilsynelatende er trygghetsskapende for borgerne, men likevel svekkes enkeltes rettssikkerhet. Straffesakssystemene er nødvendige registre som skal fungere som verktøy for straffeforfølgelse og forebyggende arbeid, noe som skal gi trygghet for borgerne. Det finnes svakheter ved systemene som kan svekke rettssikkerheten til enkeltpersoner, men det er svakheter som også kan få negative konsekvenser for politiet. Politiet har heller ingen fordeler

av disse svakhetene. Etter mine funn er ikke straffesakssystemene noe politiet har *tilsynelatende* for borgernes sikkerhet, det *er* for borgernes sikkerhet. Det er også i aller høyeste grad nødvendig for politiet å ha systemene for å kunne løse sine arbeidsoppgaver, selv om systemene ikke bidrar til effektiv oppgaveløsning.

Flyghed (2003: 74) mener at det i dag er flere trusler og mer som oppfattes som trusler enn tidligere. Et trusselbilde kan skape frykt som man på forhånd ikke vet hvor begrunnet er, fordi man ikke vet om truslene er reelle eller potensielle (Flyghed, 2003: 78-79). Ekspertene skal diagnostisere hvilke farer vi står ovenfor i fremtiden, men Flyghed poengterer at mange trusselvurderinger viser seg å være helt feil i ettertid. Før intervjuene lurte jeg på om politiets risikovurderinger også viste seg å være feil, og hva som ofres for å ivareta at den eventuelle risikoen ikke slår ut. Jeg har allerede drøftet noe av dette. For det første har jeg ikke funnet den type risikovurderinger jeg antok at fantes, nemlig vurderinger av konsekvenser av risikoene knyttet til kvaliteten på straffesakssystemene slik de er i dag, og sannsynligheten for dette. For det andre mener jeg at politiet ikke har noe valg når det gjelder å ha straffesakssystemene. De må leve med tungvinte og gammeldagse systemer som vanskeliggjør deres jobb for i det hele tatt ha noe som helst av informasjon om lovbrøyttere. Dermed er det politiets tid som ofres. Når det foreligger risikoer knyttet til verktøyene, er det først og fremst et hinder for at politiet kan utføre sine arbeidsoppgaver tilfredsstillende. Hva informantene legger i rettssikkerhet er ulikt, men både for politiets skyld og for publikums skyld er det en IKT-situasjon som bør endres.

5. Risikoenes betydning for publikum og publikums tillit til politiet

Politiet har myndighet til å utøve makt, men det forutsetter tillit fra innbyggerne (Politianalysen, 2013: 156-167). I dette kapittelet skal jeg drøfte hvordan publikum kan tenkes å bli påvirket av risikoene ved straffesakssystemene, og publikums tillit til politiet.

5.1 Rettssikkerhet

Som diskusjonen i forrige kapittel viste, har jeg identifisert risikoer for at rettssikkerheten kan svekkes på enkelte områder. Det er den lave brukervennligheten, straffelovens manglende ikrafttredelse og at systemene ikke kommuniserer med hverandre som er de risikofaktorene som kan føre til svekket rettssikkerhet hvis begrepet forstås i sin klassiske forstand. Forstås rettssikkerhet ved at den kun gjelder overgrep fra staten, er det de manglende funksjoner for sporing og logging som er de risikofaktorene som kan føre til svekket rettssikkerhet. At rettssikkerheten kan svekkes, betyr ikke at den er svekket. Det er ikke nødvendigvis slik at staten utnytter situasjonen, og misbruker sin maktposisjon. Det er heller ikke sikkert at borgerne utnytter de mulighetene de får til misbruk gitt identitetsproblematikken.

Etter å ha snakket mye om risikoene knyttet til straffesakssystemene, spurte jeg informantene om situasjonen kan svekke rettssikkerheten. Poenget med å knytte risiko opp mot rettssikkerhet er å få et bilde av situasjonens betydning for publikum. Dessverre ba jeg ikke informantene forklare hva de la i begrepet rettssikkerhet selv om vi snakket om hvordan risikoene knyttet til straffesakssystemene kan tenkes å påvirker rettssikkerheten. Jeg spurte brukeren om man kan si at dagens situasjon svekker rettssikkerheten. Brukeren svarte: «Ja, det er jo helt klart. Når man ikke kan bruke ny straffelov, og tiden det tar å registrere, og de som er ute må inn for å skrive ... Det er jo et lite effektivt og lite tilgjengelig politi.» Når informanten sa at de som er ute må inn for å skrive, siktes det til patruljerende politi som må inn på stasjonen for å skrive rapporter. Den siste tiden er det gjort tiltak mot dette i form av at flere distrikter har fått nettbrett med lese- og skrivetilgang i flere av politiets systemer som de kan ha med ut fra stasjonen (Politianalysen, 2013: 202). Sitatet fra brukeren viser en vid forståelse av rettssikkerhetsbegrepet. Publikum rammes ved at den nye straffeloven ikke er trådt i kraft. De kan, for eksempel, bli utsatt for terror uten at siktede blir dømt etter den strafferammen som finnes i det nye lovverket. Publikum rammes også ved at politiet må inn

for å skrive rapporter, og er mindre tilgjengelig enn om de var ute. På den andre siden er også rapportskrivningen en del av forebyggingsarbeidet.

Straffesakseksperten ville ikke si at det er svekket rettssikkerhet, men sa: «At vi ikke har velfungerende IKT-systemer fører til at vi ikke får utført de tjenester som vi skal. Det fører til utrygghet for deg og meg.» Utrygghet er ikke nok for å hevde at rettssikkerheten svekkes, men i det utryggheten får rot i en virkelig hendelse, i form av at man blir offer for en straffbar handling, så kan man hevde at rettssikkerheten er svekket.

Systemspesialisten sa: «En fornying er på sin plass, men jeg vil ikke kalle det en IKT-krise». Jeg spør informanten om det foreligger risiko som kan gå ut over rettssikkerheten. «Vi håndterer det meste, ellers ville vel riksadvokaten vært på banen for lengst, tenker jeg.» Svaret kan tyde på at informanten forventer at riksadvokaten har full oversikt over risikoene knyttet til straffesakssystemene. Noe som kanskje ikke er realistisk når det ikke finnes systematiske risikoanalyser.

Systemspesialisten fortalte, som jeg skrev i kapittel 4.2 at det er fatalt hvis noe skjer med stormaskinen som driver Strasak, men vedkommende sa at det ikke er en IKT-krise eller fare for svekket rettssikkerhet: «Så lenge stormaskinen ruller og går, er den helt bruknes.»

Informantene var enig om at noen problemer er større enn andre, for eksempel er det at straffeloven ikke kan tre i kraft alvorlig, men informantene hadde ulik oppfatning av hvor dramatisk dagens situasjon egentlig er. Brukeren mente situasjonen var ille.

Straffesakseksperten sa at mange vil si at rettssikkerheten er svekket, men informanten ville ikke sette noen karakter på det. Systemspesialisten så behovet for nye systemer, men syntes ikke dagens situasjon var uholdbar. Juristen, som kanskje har minst erfaring med bruk av systemene, mente situasjon ikke var dramatisk. Dette kan tyde på at jo mer systemene brukes, jo mer preget blir brukeren av situasjonen, og synes derfor den er ille.

Jeg mener at straffesakssystemene ikke bidrar til svekket rettssikkerhet alene, men jeg kan heller ikke si at de bidrar til å opprettholde sterk rettssikkerhet. Nye systemer som er bedre tilrettelagt for brukerne, vil trolig gi et bedre utgangspunkt for høy rettssikkerhet uansett forståelsen av begrepet.

5.2 Datasystemer, kontroll og tillit

Skirbekk (2012) skriver at det generelt er høy tillit i Norge. Han forsøker å si noe om hvorfor vi har tiltro til hverandre og viser til undersøkelser som finner at vi er verdens mest tillitsfulle folk. Noen mener tilliten strekker seg så langt at vi er naive (Skirbekk, 2012: 12-13). Det er flere måter å forstå tillit på. Det kan være noe vi tar for gitt eller det kan være noe man går inn i etter nøye overveielser (Skirbekk, 2012: 18). Forståelsen av tillit beror også på hva slags samfunn man lever i. Ifølge Skirbekk er det en utbredt internasjonal forståelse at det kun er mulig å ha tillit til personer. Grimen mener det også er mulig å ha tillit til institusjoner (Grimen, 2012: 86). De som mener det ikke er mulig å ha tillit til institusjoner, argumenterer med at tillit kun kan gis aktører fordi det bare er aktører som kan gjengjelde tilliten (Grimen, 2012: 96). Jeg skal ikke ta denne diskusjonen her, men jeg ønsker å vise at det er et delt syn på om det er meningsfylt å snakke om tillit til institusjoner. Jeg mener det er mulig å ha tillit til institusjoner. Grunnen til det er at en organisasjon gjerne har et samlet sett verdier og mål som det jobbes mot. Utføres organisasjonens oppgaver slik det forventes, gitt verdiene og målene, så er organisasjonen tillit verdig. Samtidig er det kanskje menneskene i institusjonen som er de egentlige bærerne av tilliten, men det er resultatet av det institusjonelle fellesskapet en utenforstående eventuelt har tillit til. Det kan være meningsfylt å dra tillitsspørsmålet enda lenger; er det mulig å ha tillit til datasystemer? Dette kommer jeg tilbake til senere.

I Norge forventer borgerne at rettsvesenet tar vare på borgernes rettigheter, men en som har tillit til en annen setter seg selv i en sårbar posisjon. Vi forholder oss til profesjonelle og institusjoner ved at de ivaretar informasjon om oss, og dermed får de en type makt over oss. Den sårbare posisjonen er reell og utgjør en risiko (Grimen, 2009: 27-29). Som tillitsgiver må det tas forholdsregler, og det er ofte et skjønsspørsmål hva som er tilstrekkelig mengde forholdsregler. Når det gjelder å stole på institusjoner, er det ofte uten å ta forholdsregler fordi det er få forholdsregler å ta (Grimen, 2009: 32). Politiet er en type institusjon som har informasjon om borgerne som borgerne må forvente at politiet ikke misbruker. Ifølge Skirbekk (2012: 18) er man sårbar når man er tillitsfull, men man slipper å bruke mye energi på forholdsregler og kontroll. Borgernes relativt høye tillit til politiet, som jeg kommer til i kapittel 5.4, er en potensiell årsaksforklaring på hvorfor politiet ikke har gjort noe med de utdaterte straffesakssystemene før. Borgerne har få eller ingen muligheter til å ta forholdsregler på dette feltet, med unntak av kontroll fra datatilsynet. Derfor er det ikke nødvendig for politiet å gjøre noe med utfordringene av tillitshensyn. Grimen skriver at

enkelte forskere hevder at staten har så mye makt at borgerne ikke kan ha tillit til den. I tilfeller med absolutt makt er dette riktig, men ellers blir det en litt for enkel påstand, ifølge Grimen (2009: 52). Det er en asymmetrisk relasjon mellom partene hvis den ene skal ivareta den andres interesser uten å få noe igjen. Kunnskap som den ene part besitter, som den andre part ikke har tilgang til, skaper også en skjev balanse hvor tillitsgiveren må velge å stole på tillitsmottakeren. En tillitsgiver utsetter seg for reell fare fordi han ikke kan vite hva tillitsmottakeren vil gjøre i fremtiden. Som borgere tvinges man inn i denne faren ettersom man har få eller ingen alternativer enn å stole på staten (Grimen, 2009: 54-66). Boe (1993: 376) skriver at det å vite mye om andre gir en maktposisjon som setter krav til at rettssikkerhet og systemsikkerhet prioriteres. Hvis publikum får vite at systemene er velfungerende og den registrerte informasjonen er kvalitetssikret, kan det gi økt tillit.

Så var spørsmålet om det er mulig å ha tillit til datasystemer. Det betyr at det må stoles på at institusjonen har gode rutiner for intern kontroll. Når det stoles på teknologi, gjelder det kvaliteten til et arbeid. Hvis det stoles på informasjonen i registre, stoles det på at den som har lagt informasjonen inn i systemet har vært ærlig (Grimen, 2009: 81). Kontroll er en måte å ta forholdsregler på, men det krever igjen tillit til kontrolløren (Grimen, 2009: 88). Folket vet ikke alt om en institusjon eller de som jobber der, men må satse på at de har motiver for å være pålitelige og at de er forutsigbare (Grimen, 2009: 111). Borgerne må også stole på at den interne og eksterne kontrollen fungerer (Grimen, 2009: 117). Dette betyr at tilliten til politiet gjelder flere ledd. Det må stoles på at informasjonen som ligger til grunn for registrering er korrekt, at den som registrerer gjør det riktig, at systemene fungerer slik de skal og at registrert informasjon ikke misbrukes.

Brukeren mener at mer kontroll og kvalitetssikring kunne bedret registreringene. Informasjonsteknologi stiller krav til kontrolltekniker og økt kontrollkapasitet. Selv om kontroll oppfattes av mange som noe negativt mener Schartum at kontroll må sees som nødvendig og legitimt når det foregår i regi av rettsstaten. Han sier også at det kan være til fordel for borgerne å være under kontroll (Schartum, 1997: 51). «Det må derfor være bedre å være aktiv deltaker ved behandlingen av egne saker og derfor være gjenstand for kontroll, enn å være en passiv tilskuer, fri for kontrolltiltak» (Schartum, 1997: 66). Når brukeren etterspør mer kontroll og kvalitetssikring er det intern kontroll og ikke kontroll av borgerne som Schartum skriver om. Poenget til Schartum er likevel relevant. Politiet må se kontrollen som

nødvendig, og borgerne får gevinst i form av økt rettssikkerhet fordi det blir mindre sannsynlig at feil utføres fra staten sin side.

Schartum spør om de manuelle delene av saksbehandlingen er mer sårbare for feil enn de automatiserte og om kontrollen derfor må rettes til det manuelle arbeidet, eller om det er omvendt. Den største forskjellen mellom de to feilkildene er at feil som oppdages innenfor automatisert saksbehandling kan rettes, og forblir rettet i fremtidige tilfeller. Feil i manuell saksbehandling derimot kan ikke rettes for fremtidige saker. Samme person kan gjøre samme type feil igjen eller det kan være andre personer som gjør den samme feilen (Schartum, 1997: 62). Ut i fra denne argumentasjonen mener Schartum at kontroll bør settes inn mot automatiserte rutiner fordi gevinsten der er størst, men at det ikke kan gå på bekostning av kontroll av manuell saksbehandling. Sistnevnte gir grunnlag for å vurdere skjønnsbaserte avgjørelser, og er derfor like viktig (Schartum, 1997: 63). Mer om kontroll blir det i kapittel 6.3 hvor det diskuteres i sammenheng med maktanvendelse gjennom datasystemer.

5.3 Å skape tillit

Tillit til systemer blir institusjonalisert gjennom lover, regler, rettigheter og plikter (Et ansvarlig politi, 2009: 36). Hva skjer da når systemene ikke fyller de kravene loven stiller, slik det er med dagens straffesakssystemer og politiregisterloven? Da ligger ikke situasjonen til rette for å skape tillit. I Et ansvarlig politi (2009: 178-180) anbefales åpenhet og tydelighet overfor publikum for å skape tillit. Manglende informasjon kan føre til skepsis og svekke tilliten. Videre anbefales tydelig profilering i offentligheten, økt innsynsrett og mer offentliggjøring og informasjon på hjemmesidene (Et ansvarlig politi, 2009: 183). Etter uheldige hendelser reagerer politiet gjerne med nye rundskriv og instruksjoner, men det gir lite læring (Et ansvarlig politi, 2009: 191). Derfor foreslås det å innføre et etatsovergripende system for erfaringslæring, ikke bare av enkeltsaker, men for å se ulike tilfeller i sammenheng (Et ansvarlig politi, 2009: 186).

Tidligere har sentrale ledere i politiet måttet tåle kritikk for å holde tilbake informasjon fra offentligheten. I 2010 leverte Accenture en rapport på oppdrag fra Politidirektoratet, som fastslo mange av de samme manglene som Politianalysen har trukket frem (Rapport fra 22.

juli-kommisjonen, 2012: 333). Accenture-rapporten var lenge unntatt offentlighet, men er nå tilgjengelig for allmenheten. Fortsatt er enkelte deler av rapporten sladdet slik at det ikke er mulig å se hva som står der. Hemmeligholdelse av informasjon, slik Accenture-rapporten er et eksempel på, er ikke med på å skape tillit. Sladdet tekst bevisstgjør leseren på at informasjon holdes tilbake og det kan føre til skepsis. Det kan til og med tenkes at skepsisen som oppstår er større enn den skepsisen som ville oppstått om leseren fikk vite den hemmelige informasjonen. Sladdet informasjon legger også opp til at leseren gjetter på hva som står. Det kan føre til at usanne rykter oppstår. Jeg mener politiet har mye å vinne på mer åpenhet. Samtidig er det forståelig at politiet ikke kan være så åpne at deres metoder ikke lenger vil fungere.

Å bygge tillit er ikke lett. Grimen mener det er fire avgjørende spørsmål som må løses for at en institusjon skal fremstå troverdig.

Hvordan gjøre det rasjonelt for dem som arbeider i institusjonen å forfølge institusjonens målsettinger, og ikke bare sine egne? Hvordan få mennesker til å holde løfter, fortelle sannheten og andre ting, spesielt når dette er påkrevd fra institusjonens synspunkt, men ikke nødvendigvis rasjonelt fra individets synspunkt? Hvordan begrense omfanget av feil og misbruk? Hvordan fremstå utad som en attraktiv institusjon? (Grimen, 2012: 91)

Grimen skriver at gode institusjoner er pålitelige og har gode mekanismer for det han kaller intensivsystemer. En risikoanalyse vil være en form for intensivsystem. Grimen mener at internkontroll avlaster publikum fra å ta forholdsregler, men når det gjelder politiet har de en makt som setter publikum i den situasjonen at det er få forholdsregler å ta. Når man har tillit til noen er man sårbar, men ifølge Grimen (2012: 88) er det to måter å redusere sårbarhet på. Det ene er at tapets størrelse kan reduseres, og det andre er at faren for tap kan begrenses. Med offentlige risikoanalyser blir det lettere for publikum å se hvordan man kan bruke de to tiltakene for å unngå sårbarhet. I stedet for å skjule risikofaktorene ved straffesakssystemene for publikum, kan det tenkes at politiet kan vinne tillit ved mer åpenhet. Det kan gjøres ved å forklare nytten av bedre systemer og lage offentlige risikovurderinger. Ved siden av en systematisk fremlegging, kan det legges ved informasjon om planlagte tiltak. Dette for å synliggjøre hva politiet ser som uakseptabel risiko og vise at det håndteres. I tillegg er risikovurderinger noe som enkelt kan fremstilles skjematisk og tydelig begrunne hvilke

beslutninger som er tatt. Disse kan være offentlige som et tiltak for å skape mer tillit. Risikoanalyser vil på den måten fungere som et kontrollsystem. På denne måten kan politiet vise at de har kontroll over risikoene, og at de har gjennomtenkte tiltak som kan settes inn. Publikums tillit vil trolig øke hvis politiet gjennomfører kontroller (Skirbekk og Skirbekk, 2012: 69).

En institusjon er pålitelig hvis personene som jobber der er pålitelige og følger institusjonenes verdier (Grimen, 2012: 97). Tall fra spesialenheten viser at de behandlet 1418 anmeldelser i 2013. Av disse ble 6 prosent avgjort med positiv påtale som vil si forelegg eller at det ble tatt ut tiltale, men hvor saken ikke er avgjort enda (Årsrapport 2013: 30). 6 prosent tilsvarer 81 av anmeldelsene. Tallene viser at det kan være en og annen utstikker i etaten, men generelt er politiet pålitelig. Da spiller det kanskje ikke noen rolle, for publikums tillit, om straffesakssystemene er utdaterte. Selv om det er risiko ved straffesakssystemene, er det fortsatt grunnlag for at publikum kan ha høy tillit til politiet. Dette fordi politiet har gode verdier, og kanskje har de funnet svarene på spørsmålene Grimen mener er avgjørende for troverdighet. Selle og Wollebæk (2012: 175) er ikke helt enig med Grimen. De argumenterer for at det ikke er tilstrekkelig å være en god institusjon for å skape tillit. Institusjonen er avhengig av å befinne seg i et sterkt sivilsamfunn, slik vi har i Norge. Et sterkt sivilsamfunn skaper muligheter og synliggjør at samhandling er rasjonelt og funksjonelt (Selle og Wollebæk, 2012: 192). Det burde være mulig for politiet i Norge å tilegne seg tillit i befolkningen, men i tesen min antar jeg at IKT-situasjonen er med på å svekke tilliten. I neste delkapittel viser jeg til undersøkelser om tillit til politiet som motbeviser min tese.

5.4 Publikums tillit til politiet

Jeg spurte informantene om hvordan dagens IKT-situasjon påvirker publikums tillit til politiet. Riktignok kan medias fremstilling påvirke hvordan publikum oppfatter politiet, og mediene velger gjerne å presentere avvikshistoriene om feil eller overtramp begått av politiet fordi det selger godt (Reiner, 2003: 275-276). Likevel har media klart å lage et bilde av politiet som beskyttere fordi de først og fremst trykker mange alvorlige saker som politiet faktisk løser (Reiner, 2003: 268). Informantene mener at publikum ikke er så interessert i politiets IKT-situasjon, og at de er mest opptatt av å få anmeldt og oppklart egne saker. De

tenker ikke på sammenhengen mellom bedre straffesakssystemer, bedre forebygging og høyere oppklaringsprosent, som straffesakseksperten vektlegger.

Hvis det er sammenheng mellom straffesakssystemene og hvor mye tillit publikum har til politiet, kunne det være ønskelig for politiet at publikum ikke fikk vite om risikoen ved straffesakssystemene. Informantene er imidlertid enige om at risikoene bør være kjent for alle fordi kunnskap gir politisk vilje til å gjennomføre endringer. Endringer som er svært etterlengtet og som vil gi gevinst både for politiet og publikum. Brukeren trekker også frem en annen grunn: «Hovedsakelig er IKT-systemene et politianliggende, men alle bør vite om situasjonen fordi det gjelder mange. Når vi snakker om risiko og straffeattester, så er jo det viktig for alle. De som skal jobbe med barn må ha attester, og det er jo ikke bra hvis det er feil da.» Selv om publikum vet at politiet har risikoelementer knyttet til straffesakssystemene, hindrer ikke det en voldtektsmann å bli ansatt i barnehage. Publikums kjennskap kan likevel bidra til at penger bevilges, og at politiet ikke kommer i samme situasjon igjen. Dette kan igjen bidra til at politiet kan løse sine oppgaver på en mer effektiv måte.

Innbyggerundersøkelsene er undersøkelser av den norske befolkningen foretatt på oppdrag fra direktoratet for forvaltning og IKT (Difi). Undersøkelsene tar for seg innbyggernes og brukernes tilfredshet av statlige, kommunale og fylkeskommunale virksomheter. De som har deltatt i undersøkelsen deles i to grupper. Den ene omtales som brukere og den andre som innbyggere. Brukerne er de innbyggerne som har benyttet seg av eller vært i møte med virksomhetene, mens innbyggerne er både brukere og personer som ikke har noen erfaring med virksomhetene (Innbyggerundersøkelsen). Undersøkelsene sier noe om borgernes tillit til virksomhetene. Svært tilfredse borgere har sannsynligvis høy tillit, mens mindre tilfredse borgere har mindre tillit.

Skåren i undersøkelsen går fra 0-100 og anbefalt tolkning av skåren er: 0-50 *nøytral eller misfornøyd*, 51-70 *delvis fornøyd*, 71-80 *fornøyd*, 81-100 *svært fornøyd*. For politiet sin del viser innbyggerundersøkelsene en skår på 58 i 2010 og 60 i 2013, blant innbyggerne. Altså har det vært en liten økning. Blant brukerne er skåren på 69 i 2013, mens jeg ikke har funnet tall for brukerne fra 2010. Tallene viser at de som har vært i kontakt med politiet har høyere tillit til dem enn de som ikke har vært i kontakt med politiet (Innbyggerundersøkelsen). I sin

analyse vurderer Difi politiets skår til at befolkningen har høy tillit til politiet (Difi rapport). Likevel er det fortsatt 30 skår å gå på for å vinne mer tillit.

TNS Gallup har på oppdrag fra Politidirektoratet også gjennomført undersøkelser om tillit til politiet. I Politiets nasjonale innbyggerundersøkelse (2010: 16) konkluderes det med det motsatte av Difi sine innbyggerundersøkelser. Nemlig at det er de som har vært i kontakt med politiet som har klart minst tillit til etaten. De som hadde vært i kontakt med politiet og hadde lav tillit til dem, begrunnet den lave tilliten med kritikk av politiets prioriteringer, henlagte saker og politiets tilgjengelighet. Runhovde (2010: 196) mener at dette kan forklares med befolkningens urealistiske forventninger, og kritikkverdige handlinger fra politiet. Hun mener imidlertid det er uheldig at de som har vært i møte med politiet opplever å bli skuffet. Politiets nasjonale innbyggerundersøkelse (2010: 16) viser at de som har mest tillit til politiet er kvinner, personer under 30 år, personer med høy utdanning og personer som ikke har vært utsatt for noe kriminelt eller har hatt erfaringer med politiet. I Politiets nasjonale innbyggerundersøkelse (2010: 13) kommer de frem til at 86 prosent av befolkningen har tillit til politiet, noe som er en økning på 3 prosent siden 2008. De fleste, 68 prosent, av de som har tillit til politiet, anser tillitsnivået som *stor* når de kan velge mellom alternativene *svært liten*, *liten*, *stor* og *svært stor*.

I Innbyggerundersøkelsen får politiet skryt for sin bruk av sosiale medier. Etaten er aktiv både på twitter og facebook, men det er vanskelig å tolke undersøkelsen mot min oppgave. Publikum har ikke direkte kontakt med straffesakssystemene, og derfor har de heller ikke mulighet til å bedømme dem spesifikt. Undersøkelsen spør heller ikke om straffesakssystemene. Det er spørsmål om digitale tjenester, men det er de tjenester publikum selv kan bruke. Det blir derfor feil å sammenligne med det. Derimot spør undersøkelsen om politiets evne til å løse oppgaver. Blant brukerne er skåren for oppgaveløsning 68. I det inngår kompetanse til å løse oppgaver, evne til å informere om rettigheter, evne til å hjelpe i en nødsituasjon, evne til å løse konflikter eller ubehagelige situasjoner, evne til å møte publikums behov i uvanlige situasjoner, evne til å følge opp brukerne, evne til å gi råd og evne til å forebygge kriminalitet (Innbyggerundersøkelsen). Straffesakseksperten mener at straffesakssystemene kan påvirke politiets evne til å løse sine oppgaver effektivt. Gjennom å se på den anbefalte tolkningen av skåren, fremkommer det at publikum er *delvis fornøyd* med politiets evne til å løse sine oppgaver. Skåren ligger på 60 for forebygging. Den kunne vært høyere, men samtidig er den relativt høy.

Runhovde skriver at politiet er avhengig av tillit fra befolkningen for å kunne samarbeide med dem og for å få aksept for sine maktutøvende handlinger. Hun mener også at tillitsnivået kan forstås som en indikator på kvaliteten av politiets arbeid (Runhovde, 2010: 190). Videre trekker Runhovde frem flere måter å operasjonalisere tillit på: «Man kan ha tillit til at 1) politiet kommer når en ringer, 2) at de vil gjøre sitt beste for å hjelpe en, 3) at kriminelle blir straffet, 4) at alle får likeverdig behandling fra politiet, 5) at politiet opptrer ifølge loven osv.» (Runhovde, 2010: 191). Hun påpeker at det ikke finnes alternative instanser innen samme område og at publikum derfor tvinges til å benytte seg av politiet i enkelte sammenhenger. I andre sammenhenger finnes det private selskaper som tilbyr tjenester som kan konkurrere med politiets tilbud. Derfor må man ha det manglende alternativet for tilsvarende tjenester i bakhodet når man skal forstå tillitsundersøkelsene som viser at politiet har høy tillit i befolkningen (Runhovde, 2010: 193-194).

I tesen som ble presentert i innledningskapittelet skrev jeg blant annet at risikoene ved straffesakssystemene kan tenkes å påvirke publikums tillit til politiet. Det er vanskelig å bevise eller motbevise. Innbyggerundersøkelsene viser at borgerne har relativt høy tillit til virksomheten, men så har ikke undersøkelsen hatt noen spørsmål som angår straffesakssystemene. Publikum har heller ikke et godt grunnlag for å mene noe om systemene. Systemene inneholder informasjon som er avgjørende for politiet, men det er vanskelig for publikum å se når og hvordan informasjonen brukes. Hvis noe av risikoen rammer enkeltpersoner på en negativ måte slik at de føler det som et overgrep fra staten, altså et direkte brudd på rettssikkerheten, vil de sannsynligvis si ifra, og det vil bli ordnet opp i. Slike tilfeller vil det uansett være relativt få av. Det vil derfor ha liten påvirkning på resten av befolkningens tillit til politiet.

Juristen mener at man må ha tillit til politi og myndigheter fordi det er de som beviselig har gjort noe galt tidligere som er mistenkelige og det er i liten grad staten. Informanten tror at det er en skepsis blant borgerne som ikke har rot i det samfunnet vi lever i. Nå viser innbyggerundersøkelsen at det faktisk er relativt høy tillit i befolkningen så kanskje bedømmer juristen borgerne feil. Poenget juristen vil ha frem er dog at mer registrert informasjon ikke vil være et onde for den enkelte. Mange er kanskje redd for myndigheters

misbruk. Juristen påpeker at det er mer misbruk av statlige goder fra borgernes side, enn det er misbruk av informasjon fra statens side.

Wollebæk, Enjolras, Steen-Johnsen og Ødegård (2012) utførte tillitsundersøkelser i etterkant av 22. juli for å se hvordan tilliten ble påvirket av de dramatiske hendelsene. Undersøkelsene viste at tilliten til institusjoner økte i tiden etter angrepet. Ett år etter var tilliten tilbake på det nivået den hadde vært i forkant av 22. juli. Tillit kan påvirkes av store hendelser, men Wollebæk m.fl. mener at det stort sett er på kort sikt. Ellers holder tillitsnivået seg på et jevnt nivå. Sammenlignet med tillitsnivået ellers i verden, har vi et høyt tillitsnivå her til lands (Wollebæk m.fl., 2012: 42). Tilliten til politiet spesielt, avviker noe fra de andre institusjonene Wollebæk m.fl. skriver om. De første månedene etter angrepet var tilliten til politiet høy, men etter at 22. juli kommisjonsrapporten ble lagt frem sank tilliten fra 82 til 69 prosent. Før hendelsene var tallet 77 prosent. Befolkningen hadde minst tillit til PST, politiets ledelse og politiets administrasjon (Wollebæk m.fl., 2012: 44-45). Eriksen skriver om hvordan en institusjon kan reparere mistillit. Han foreslår å bruke årsaksanalyser for å finne de beste og mest rasjonelle virkemidlene (Eriksen, 2012: 220). I neste kapittel vil jeg ta for meg mulige årsaksforklaringer for politiets situasjon med utdaterte straffesakssystemer i et forsøk på å finne rasjonelle tiltak.

6. Årsaksforklaringer og mulige tiltak

Det er relevant å spørre hvordan straffesakssituasjonen har blitt slik den er i dag for å unngå å komme i samme situasjon igjen. Det er ikke noe enkelt svar på dette ettersom det er sammensatte grunner til at straffesakssystemene er umoderne og risikofylte, men det er likevel relevant å diskutere. Denne oppgaven er for liten for å gå skikkelig i dybden på mulige årsaksforklaringer, men en liten drøftelse blir det. Mulige tiltak som kan settes inn for å unngå å komme i samme situasjon igjen skal også drøftes. Da tenker jeg på når de nye systemene er på plass. Hvordan sikre at de ikke blir umoderne og fylt med de samme risikofaktorene som finnes i dag? Er det noe verden har sett de siste 20 år, er det hvor fort teknologi videreutvikler seg. Det er derfor helt sentralt at politiet fortsetter å fornye systemene sine slik at de blir nyttige verktøy som kan imøtekomme lovverk og arbeidsoppgavene til etaten.

Straffesakseksperten fortalte at de lager systemer som det er lettere å gjøre endringer i enn det er i dagens systemer. Mens man venter på MERVERDIprogrammet er det kanskje andre tiltak som kan settes i gang. Straffesakssystemene skal tross alt brukes i noen år til. I dag blir ikke tidsbruk på enkeltoppgaver registrert. Hva politiet bruker tiden sin på blir ikke analysert på en helhetlig og regelmessig måte (Politianalysen, 2013: 78). Dermed blir det vanskeligere å finne forbedringsområder og tiltak, men noe er likevel mulig å gjøre. For at den nye straffeloven skal kunne tre i kraft er det behov for flere tiltak, men tiltak i forbindelse med dette skal ikke jeg diskutere da det er for datateknisk komplisert.

Helt siden begynnelsen av 2000-tallet har det vært snakk om at det skal lages nye straffesakssystemer. Juristen mener at fordi man har klart å lappe på det gamle underveis, har man ikke sett det store behovet for nye løsninger. IKT har ikke, før nå, vært høyt prioritert i politiet (Politianalysen, 2013: 192). Som jeg har vist i denne oppgaven, er behovet for fornyelse absolutt til stede. Den nye straffeloven ble vedtatt i 2005, og loven synliggjorde behovet for nye straffesakssystemer for politikere og publikum. I juli i år trer politiregisterloven i kraft. Den vil tydeliggjøre det rettslige behovet ytterligere da dagens systemer ikke imøtekommer lovens krav. Det kan diskuteres om det er akseptabelt at det tar så lang tid før det kommer nye systemer, men enda viktigere er det å kartlegge hvorfor politietaten har kommet i den situasjonen at behovet er såpass prekært. Under intervjuene snakket vi om ulike årsaksforklaringer til hvordan politiet har havnet i en situasjon som gjør at det er behov for *Nybygg*. Svarene til informantene varierte. Jeg tok opp forklaringer som

kultur, ledelse, organisering, politikk og ressurser. Dette er store temaer som denne oppgaven ikke går i dybden av, men det er likevel viktig å si noe om det. I Politianalysen (2013: 9) konkluderes det med at politiet har manglet nødvendige rammevilkår for å styre etaten best mulig, samtidig som de heller ikke har klart å gjøre noe ut av de mulighetene de har hatt. Utvalget mener at det har vært svak teknologiledelse, og at etaten har for dårlig teknologiunderstøtte.

6.1 Politiets organisering

Følgende beskrivelse fra Politianalysen viser utfordringene ved å være en offentlig virksomhet:

Offentlig virksomhet er politisk styrt, og å utøve ledelse i det offentlige har noen spesielle særtrekk. Virksomhetene i offentlig sektor kjennetegnes av stor oppgavebredde og situasjonsmangfold i oppgaveutførelsen. Det stilles også ofte krav til hvordan oppgavene skal utføres. Antall interessenter er større og relasjonen mellom virksomheten og omgivelsene er ofte mer kompleks enn i andre virksomheter. Dette gir andre rammebetingelser og et mer krevende utgangspunkt for å sette mål, definere rammer og måle resultater. Kvaliteten på den tjenesten som skal leveres, vil videre avhenge av samarbeid og kompromiss med andre aktører som har andre formål og andre hensyn. Dette stiller krav til en annen grad av helhetlig konsekvenstenkning og samarbeid. En annen begrensende rammebetingelse i offentlig sektor er de årlige budsjettildelingene. Budsjetter som fastsettes for ett år av gangen, kan føre til usikkerhet om fremtidige rammer og vanskeliggjøre langtidspanlegging (Politianalysen, 2013: 156).

For å håndtere noen typer risiko, har det moderne samfunn utviklet avtaler i form av lover, kontrakter og forsikring. Når disse utformes må det risikovurderes for at de skal bli gode. Risikovurderingen består i, som nevnt tidligere, å se på sannsynligheten for tap og graden av det eventuelle tapet. Det som utgjør risiko for én person, utgjør ikke nødvendigvis risiko for en annen (Luhman, 1993: 72). Risikable beslutninger og avgjørelser tas ofte av makthaverne i den politiske verden. Politikere kjenner ikke fremtiden, men de kan presentere beslutninger som risikable, og vise at de har undersøkt alternativene og valgt det alternativet som kom best ut (Luhman, 1993: 155-156). Mange næringer skylder på politikerne hvis noe ikke går som det skal. Det politiske systemet innebærer en aksept av at mindretallet må bøye seg for flertallet. «Innenfor rammen av det demokratiske system er politisk makt et verdiprinsipp som

slår igjennom i forhold til ulike alternative beslutningsformer i den politiske beslutningsprosess» (Bernt og Doublet, 1999: 415).

Alle fire informantene peker på organiseringen til politiet med den politiske styringen der Justis- og beredskapsdepartementet er plassert på toppen, som mulig årsaksforklaring for den manglende utviklingen innen IKT i politiet. Det er mange ledd i etaten, og selv om det hyles høyt om hvilke behov som foreligger, så når det ikke frem til beslutningstakerne.

Straffesakseksperten fortalte: «Nå har Justisdepartementet ansatt mennesker som skal arbeide med IKT i etaten og personer som skal jobbe opp imot fag. Så de har sett den koblingen, men det er først nå.» Så vidt jeg forsto informanten, mente vedkommende at det er de samme personene som skal jobbe med IKT og politifag. Disse personene skal sørge for at IKT kan bli et godt verktøy for å løse faglige utfordringer og politimessige oppgaver. Ifølge informanten har ikke det vært gjort på departementsnivå tidligere. I *Analyse av IKT-styringen i politi- og lensmannsetaten* legges det vekt på at utvikling og innovasjon skal sikres i fremtiden. IKT skal understøtte oppgaveløsningen i etaten som forebyggende arbeid, kriminalitetsbekjempelse og forvaltningsoppgaver. Som informanten min sa står det også her at IKT-avdelingen i POD skal se det politifaglige og IKT-faglige sammen for å skape gode og effektive arbeidsprosesser og imøtekomme publikum og deres behov (*Analyse av IKT-styringen i politi- og lensmannsetaten*, 2013: 21).

I Politianalysen (2013: 196-197) nevnes også Politidirektoratets svake kompetanse på IKT-området. Ifølge Politianalysen har Politidirektoratet manglende strategier og kost/nytte-analyser, i tillegg til at brukernes kompetanse benyttes i liten grad. I Politianalysen (2013: 29) pekes det også på at politiets organisering gjør det vanskelig å løse kjerneoppgavene på en god måte, men de legger nok ikke helt det samme i *organisering* som mine informanter. Utvalget tenker blant annet på distriktsinndelingen, men de sier også at det har vært for dårlig sentral styring og manglende sentrale retningslinjer. Utvalget presiserer at omorganisering i seg selv ikke vil hjelpe, men en bedre organisering kan legge forholdene til rette for bedre oppgaveløsning. Det er ca. 13 000 ansatte i politiet (politi.no). Med 35 underlagte virksomheter under Politidirektoratet, er det forståelig at det er vanskelig å få til god styring (*Politianalysen*, 2013: 30).

Informanten fra PDMT fortalte om en hendelsesstyrt etat og politisk styrt organisering:

Det er jo politisk. PDMT kan ikke sette i gang ting på egenhånd. Vi er styrt av POD som igjen er styrt av JBD, så vi har jo opplevd mange ganger at statsrådene har kommet og markert seg. Så skal de ha gjennom noe med en gang, og da må vi bare gjøre det. Dette er min personlige mening. Det har jo med penger og tildeling å gjøre. PDMT venter jo på oppdrag. Det er synd det må kollapse før det gjøres noe. Det er jo ikke et sunnhetstegn.

Det informanten fortalte om, bekreftes i Politianalysen:

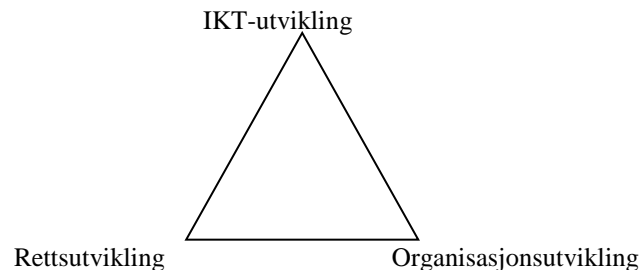
Justis- og beredskapsdepartementet og Politidirektoratet må utøve en mer langsiktig og helhetlig strategisk styring av etaten ettersom styringen i dag er preget av å være ufullstendig, hendelsesstyrt og kortsiktig. Roller og ansvar må fordeles mellom departement, direktorat, politidistriktene og særorganene, og fullmakter må stå i samsvar med det ansvaret som er tillagt de forskjellige nivåene i organisasjonen. Dette vil kunne bidra til at etatens ressurser benyttes på en bedre måte (Politianalysen, 2013: 143).

Anbefalingene som fremkommer i politianalysen er blant annet at PDMT legges ned og at funksjonene overføres til Politidirektoratet. I tillegg foreslås det at Politidirektoratet fornyer seg for å oppnå mer helhetlig styring, bedre ledelse og strategisk utvikling. IKT er en av fem punkter utvalget anbefaler at det rettes sterk oppmerksomhet mot. De andre er politifag, etatsledelse, virksomhetsutvikling og HR (Politianalysen, 2013: 142). Ansvars- og oppgavefordelingen mellom Justis- og beredskapsdepartementet og Politidirektoratet bør også tydeliggjøres da den er tåkete i dag, ifølge Politianalysen (2013: 150). Videre foreslår utvalget at IKT-utvikling blir sett som en del av den generelle organisasjonsutviklingen. Hvordan man ser på arbeidsprosessene og bruker IKT som strategisk virkemiddel for effektiv oppgaveløsning, må inngå i organisasjonsutviklingen (Politianalysen, 2013: 194). Tiltakene som foreslås i Politianalysen er delvis igangsatt. Jeg skal se nærmere på organisasjonsutviklingsmomentet.

6.2 Organisasjonsutvikling, akseptabel risiko og institusjonalisering av avvik

IKT-utvikling og organisasjonsutvikling er altså noe som bør sees i sammenheng. Samtidig spiller også rettsutviklingen inn, som straffeloven og politiregisterloven er eksempler på.

Denne modellen viser hvordan man kan se samspillet mellom retten, IKT og organisasjonen:



Figuren er hentet fra Jansen og Schartum (2007: 21).

I avslutningskapittelet trekker jeg denne illustrasjonen lenger for å vise en modell politiet kan ha enda bedre nytte av.

Chan (2001) skriver at det kan oppstå ulik forståelse av rammeverket rundt teknologiske løsninger. Brukerne har gjerne et annet syn enn utviklerne. Brukerne ønsker en lettere og mer effektiv hverdag uten å måtte endre på noe. Utviklerne er mer opptatt av at bedriften må utvikle seg sammen med systemene (Chan, 2001: 157). Teknologisk forandring kan endre organisasjoner og sosiale forhold, men teknologi skapes også av organisasjonslivet og de sosiale forholdene (Chan, 2001: 143).

Diane Vaughan er en organisasjonssosiolog som skriver om hvordan organisasjoner tilegner seg mørke sider. Hun definerer organisasjonsavvik slik: «an event, activity, or circumstance, occurring in and/or produced by a formal organization, that deviates from both formal design goals and normative standards or expectations, either in the fact of its occurrence or in its consequences, and produces a suboptimal outcome» (Vaughan, 1999: 273).

Organisasjoner er i konstant forandring, noe som kan føre til usikkerhet. Det kjempes om midler og ressurser som ofte er mangelvare. Gjennom maktkamper og mekling skapes ustabilitet i miljøet. Det kan resultere i kompromisser som ikke samsvarer med organisasjonens mål, standard og forventninger (Vaughan, 1999: 275-276). Risiko er noe fundamentalt som organisasjoner må forholde seg til, både risiko for feil og tapet som følger av feilene (Vaughan, 1999: 278). Teknologiske løsninger, som for eksempel datasystemer, er

komplekse og usikre. Derfor er de også risikable. Usikkerheten og risikoelementene er noe som kan påvirke arbeidsprosessene og bidra til feiltakelser (Vaughan, 1999: 295).

Avvik skapes gjennom manglende samsvar i rutiner, ifølge Vaughan. Hun hevder at manglende samsvar i rutiner oppstår gjennom forbindelsen mellom tre elementer. 1) Organisasjonsmiljøet. 2) Organisasjonens karakter, som struktur, prosess og oppgavesett. 3) Individene i organisasjonen og deres kognisjon (Vaughan, 1999: 274). Feiltakelser, dårlig forvaltning og katastrofer er tre mulige konsekvenser av manglende samsvar i rutine. Det organisasjonen selv som systematisk produserer avvik gjennom komplekse strukturer og prosesser, i motsetning til forståelsen om at det er noe ekstraordinært. Avviksproduseringen er organisasjonens mørke side.

Vaughan skriver at hennes syn utfordrer Webers rasjonalitetsteori i tillegg til mål - middel - tenkning fordi hun viser at en gitt atferd er rasjonell innen en gitt situasjon og en sosial kontekst. Organisasjoner opplever uforutsette negative konsekvenser som avviker fra formelle mål, standarder og forventninger, men de har skapt konsekvensene selv (Vaughan, 1999: 298).

Maurice Punch skriver om noe av det samme som Vaughan. Gjennom organisasjonssystemet fremmes og beskyttes handlinger eller tankemåter som er råtne (Punch, 2003: 172).

Mennesker som feiler kan enkelt byttes ut. Det er ikke like enkelt med avanserte datasystemer. Punch sin artikkel fremmer at det ikke alltid er snakk om ett råttent eple, men en råtten frukthage. Frukthage er en metafor for et råttent system. Punch sikter ikke til datasystemer, men til mer abstrakte, store, formelle systemer som for eksempel politiets organisasjon. Avvik i politiet kan tenkes å bli institusjonalisert, og Punch viser eksempler på grove skandaler.

Vaughan og Punch sine overføringsverdier til mitt prosjekt, handler om at politiet bruker lang tid på å komme seg ut av situasjonen med utdaterte systemer. Det gjør at problemene som foreligger kan tenkes å institusjonaliseres. Politiet tvinges til å leve med utfordringene, og lærer seg å akseptere dem. Det er mange ting som kan føre til en avvikssituasjon, blant annet mangel på kommunikasjon, samarbeid, kompetanse og informasjonsdeling (Punch, 2003: 183). Derfor er det viktig at politiet ivaretar disse elementene selv om straffesakssystemene ikke fremmer hvert element. Punch skriver at det ofte må store reformer til for å løsne opp i råtne systemer hvor reglene tøyes (Punch, 2003: 194).

I en annen artikkel drar Vaughan poenget sitt lenger, og drøfter begrepet akseptabel risiko. Hun tar for seg Challenger-ulykken i 1986. Challenger var en romferge som eksploderte bare sekunder etter at den tok av fra jordens overflate. Det tok ikke lang tid før en teknisk feil ble avslørt som årsak for ulykken, men i tillegg ble det klart at NASA som organisasjon hadde feilet. Den første og offisielle granskningsrapporten pekte på mangelfulle beslutningssystemer og faktorer som produksjonspress. Det var flere risikoelementer som ble oversett for å nå kostnadseffektive mål (Vaughan, 2004: 316).

Vaughan har forsket på Challenger-ulykken i en årrekke, og har i sine tidligere arbeider konkludert med at ulykken skyldes feil som ble begått av NASA. I denne artikkelen viser hun derimot hvordan det slett ikke var regelbrudd eller avvik som forårsaket ulykken, men noe som organisasjonen hadde gjort til en normaltilstand. NASA visste lenge at det ble begått regelbrudd, men de tok sjansen på at det skulle gå bra, og feilene ble tildekket. Det som granskingsrapporter, presse, befolkningen, og til og med Vaughan, trodde var regelbrudd viste seg senere å være innarbeidede rutiner (Vaughan, 2004: 320). Sikkerhetsrutinene var ikke brutt, men fulgt. Det var både kjent og akseptert at det forelå tekniske mangler ved romfergen. Manglene var så vanlige at de ble tatt for gitt (Vaughan, 2004: 323). Avvik ble normalisert ved at visse handlinger eller tilstander ble sett som akseptabel risiko. Det som framsto som avvik for utenforstående, var normalt og akseptabelt i NASAs kultur fordi avvikene ble normalisert. Vaughan skriver at det utviklet seg en kultur for å begå risiko og at det oppstod en strukturert form for hemmeligholdelse. «The production of culture explained how managers and engineers gradually expanded the bounds of acceptable risk, continuing to fly with known flaws; the culture of production explained why» (Vaughan, 2004: 330). Innenfor denne “produksjonskulturen” ble kompromisser mellom kost, nytte og risiko vanlig, og ikke sett på som avvik. Det var derfor konformitet og ikke avvik som førte til ulykken. Vaughan kom til en helt annen konklusjon enn granskningskommisjonen da hun fant at det var samsvar og ikke avvik som forårsaket ulykken (Vaughan, 2004: 337). Det som lenge ble sett som akseptabel risiko gikk plutselig galt. «This case was not an example of misconduct as I originally thought: rules were not violated. Still, harm was done. Moreover, NASA’s actions were deviant in the eyes of outsiders, and, after the accident, also in the eyes of those who made decisions» (Vaughan, 2004: 340).

Christin Thea Wathne har undersøkt politiets evne til å være en lærende organisasjon. Hun konkluderer med at politiet mangler omfattende strategier, og at de er for dårlig på systematisert organisasjonslæring (Wathne, 2012: 704). Det er store variasjoner i politiet når det gjelder om lederne tar ansvar for kunnskapsutvikling og stiller spørsmål som rører ved den fundamentale forståelsen av politiets verdier. I noen distrikter er de flinke og bruker systematiske måter å utvikle seg på som en organisasjon, mens andre steder er det mer fokus på enkeltindividers utvikling (Wathne, 2012: 719). Wathne mener at politiet vil tjene på å se seg mer som en enhetlig organisasjon som systematisk reflekterer over og vurderer erfaringer over tid. Samtidig skriver hun at det er vanskelig for en organisasjon å lære av kompliserte problemer som er vanskelig å håndtere (Wathne, 2012: 715). Likevel mener Wathne at ledere har stor mulighet til å påvirke kulturen på arbeidsplassen, og dermed bidra til en bedre læringskultur (Wathne, 2012: 715).

Dette delkapittelet har vist at det er forskjell mellom organisasjonsendring og organisasjonsutvikling. Organisasjoner endrer seg hele tiden, men for at det skal være positivt og utviklende må organisasjonen unngå å institusjonalisere avvik.

6.3 Ledelse og risikostyring

Ledelse handler om å styre virksomheten til å nå sine mål ved å tilrettelegge midlene (Politianalysen, 2013: 154). Det er et lederansvar å sikre utvikling av IKT til å være gode verktøy og strategiske virkemidler til å løse politiets oppgaver (Politianalysen, 2013: 204). Straffesakseksperten mener at det er ledere, helt opp til toppnivå, som ikke har sett sammenhengen mellom IKT og måloppnåelse. Alle har sittet på hver sin tue uten å ha sett hvilke gevinster som ligger i å se den store sammenhengen. Informanten vektla ledelse og innovasjon gjennom hele intervjuet, og påpekte at innovasjon ikke kan forekomme uten initiativ fra ledere. I tillegg mente informanten at det har vært lite innovativ tenking fra PDMT som databehandler, men at nåværende politidirektør Odd Reidar Humlegaard har klart å snu tankegangen mot mer innovativ og strategisk tenkning. Straffesakseksperten påpeker at det er når det går galt forståelsen om at politiet har vært for hendelsesstyrt dukker opp. Informanten sa at politiet nå er på vei mot å bli mer kunnskapsbaserte.

I Politianalysen (2013: 154) står det at utvalget har sett noen gode eksempler på ledelse hvor lokale ledere har satt i gang gode tiltak. Det er selvfølgelig bra, men det er synd at det enkelte distrikt skal finne opp egne løsninger. Det er nettopp det som skaper forskjeller og ulik praksis som igjen er uforutsigbart for publikum.

Det omfattende oppgavesettet gjør det vanskelig å være leder i politiet. Det fort gjort at jobben blir halvveis godt utført når alt må prioriteres. Dette gjør at de som sitter på toppen skyver beslutningsansvaret nedover, men beslutninger som tas langt ned i organisasjonen er ofte ikke i tråd med virksomhetens overordnede mål (Politianalysen, 2013: 155). At organisasjonen følger sine overordnede mål, er som jeg viste i kapittel 5, en forutsetning for å fremstå troverdig og vinne tillit. Da er det enda viktigere at det utarbeides gode rutiner, at det finnes god og moderne IKT-støtte og at man finner effektive og kvalitetsfylte arbeidsprosesser. Det må være god ledelse i alle ledd for å oppnå virksomhetens mål. I Politianalysen (2013: 143) står det at det er avgjørende for politiets fremtid at det settes i gang tiltak som hever styringen av etaten. Det gis anbefalinger om at etaten må styres på en mer enhetlig måte. Dette må gjøres gjennom hvordan ledere velges ut, hvordan de utvikler seg, høy kompetanse, felles opplæring og evaluering og oppfølging av lederne (Politianalysen, 2013: 161). Foster (2003: 196) mener det er vanlig i mange organisasjonskulturer å fokusere på ledelse, men at politiet er et unntak. I politiet har det vært et større fokus på operativt politiarbeid og mindre fokus på ledelse.

I 2013 ga Politidirektoratet ut en *Analyse av IKT-styringen i politi- og lensmannsetaten* som skulle gi bedre grunnlag for beslutninger rundt den fremtidige IKT-styringen. Her presenteres ulike modeller for hvordan IKT-styringen kan bli best mulig. Risiko ved de ulike modellene er vurdert, men risikovurderinger av straffesakssystemene som en del av en fornuftig IKT-styring nevnes ikke. Likevel henvises det til regler for intern kontroll og risikostyring i *Virksomhetsstyring* (2010) pkt 4.2.2. Her defineres risiko på følgende måte:

Risiko betegner forhold eller hendelser som kan inntreffe og påvirke oppnåelse av målsettinger. En risiko skal vurderes i forhold til sannsynligheten for at den inntreffer, og den konsekvens den forventes å ha. Resultatet av slik vurdering angir hvor høy den enkelte risiko er. Ledelsen må ta den endelige prioritering av hvilke risikoer som kan svekke oppnåelsen av viktige målsettinger og som således er vesentlige. Tiltak mot slik risiko skal følges opp i den løpende styringsprosessen (*Virksomhetsstyring*, 2010: 5).

Videre står det at det er virksomhetens ledelse som er ansvarlig for den interne kontrollen og at risikostyring er et sentralt verktøy.

Ved risikostyring skal virksomheten fortløpende identifisere forhold som kan påvirke måloppnåelsen, og gjennomføre korrigerende tiltak som med rimelighet kan redusere sannsynligheten for manglende måloppnåelse.

Risikostyring er et verktøy for god måloppnåelse og effektiv drift. En risikoanalyse har til hensikt å sikre:

- Målrettet og kostnadseffektiv drift
- Pålitelig intern og ekstern rapportering
- Overholdelse av gjeldende lover og regler

(Virksomhetsstyring, 2010: 12)

Sitatet viser at etaten ser nytten av risikovurderinger og skal bruke det som et verktøy for at den interne styringen fungerer som forutsatt. Det er lett å se overføringsverdien av dette til andre områder i etaten, men det gjelder å finne riktig metodikk og gjennomføre tilstrekkelig opplæring slik at risikostyring og intern kontroll kan fungere som førende prinsipper (Analyse av IKT-styringen i politi- og lensmannsetaten, 2013: 29).

6.4 Maktanvendelse gjennom datasystemer

Feeley og Simon diskuterer makt i den nye straffetenkningen. De makt Havende i samfunnet ønsker en forsikring mot og forebygging av fremtidige lovbrudd gjennom risikominimalisering. Underklassen, med minimal makt, er en gruppe som permanent ekskluderes fra sosial mobilitet og økonomisk integrasjon. De blir behandlet som en høyrisikogruppe som må kontrolleres og styres for å beskytte resten av samfunnet (Feeley og Simon, 1998: 178). Hudson mener at det er forskjell på risikostyring og risikokontroll. Hun forklarer at risikostyring gir individuell mulighet til å velge mellom gode og dårlige handlinger. Risikokontroll tar styringen lenger og fjerner valgmuligheten for handling. Det kan gjøres gjennom forbud eller ekskludering. Hudson sier at dette er en strategi som kjennetegner den nye straffetenkningen, statsstyring og neo-liberalisme. Risikostyring handler om moral og valgmuligheten for gode handlinger, mens risikokontroll fjerner muligheten til å begå enkelte handlinger og muligheten til vise god moral. Hudson ser klassifisering av risiko og risikokontroll som strategier for inkludering og ekskludering, og mener det skaper diskriminering og urett (Hudson, 2003: 75-76). Så sentralt som risikominimalisering er i

risikosamfunnet burde det kanskje gjenspeiles internt i politiet. Risikominimalisering i straffesakssystemene kan føre til mer tid til risikostyring utad. Å snu fokus fra å behandle underklassen som en høyrisikogruppe til å se på interne risikofaktorer i politiet, kan kanskje heve kunnskapen og gjøre politiet bedre rustet i møte med reell farlighet. Hudson trekker frem de negative sidene ved risikostyring og risikokontroll, men kanskje fungerer det annerledes som en form for intern kontroll enn det gjør som straffetenkning.

Douglas og Lianos (2000) skriver om hvordan samfunnet forholder seg til det som oppfattes som farlig. Som en effekt av de sosiale reguleringer er det en skapt frykt for de andre; for avvikere. Samfunnets reguleringer gjennom datasystemer med pinkoder og passord gjør at brukeren ikke kan diskutere med systemet. Det er ikke mennesker som behandler det man spør etter, men teknologiske løsninger. Systemet skiller ikke mellom god og dårlig, ond og snill, ærlig og uærlig, fattig og rik. Det eneste systemet skiller mellom er de som har og de som ikke har gyldig tilgang til det bestemte nivået (Douglas og Lianos, 2000: 7). Andre faktorer som alder, kjønn, rase og skjønnhet er også irrelevant. På den måten opplever vi en ny type sosial kontroll som ikke kan skille mellom disse tingene, og dermed ikke ekskludere på grunnlag av det. Maskiner er raske og effektive. De oppleves ikke som urettferdige, eller maktutøvende, noe som kunne vært opplevd om det var et menneske. I lys av dette tenker jeg at utdaterte straffesakssystemer kan være en måte å bruke makt på. Makten er da skjult nettopp fordi det er systemer og ikke mennesker. Maskinmakt er på den måten lettere å akseptere enn mennesker som utøver makt. Før intervjurundene lurte jeg på om politiets makt gjør at de har råd til å nedprioritere utviklingen av datasystemene sine. Ifølge informantene er det ikke politiet som har makt, det er politikerne og etatens øverste ledelse, Justis- og beredskapsdepartementet og Politidirektoratet. Dessuten har diskusjonen i oppgaven vist at situasjonen vedrørende straffesakssystemene ikke er noe som gir fordeler for politiet. Da er det lite trolig at det ligger skjult maktbruk i systemene. I løpet av intervjuene har det ikke kommet frem noen fordeler for politiet ved at situasjonen er som den er. Straffesakssystemene har bedre utnyttelsespotensiale enn de fleste brukere er klar over, men det gagnar ingen i politiet å ha dagens systemer til fordel for systemene MERVERDIprogrammet utvikler. Likevel har, som Schartum skriver, de som lager kodene i systemet en viss makt fordi kodene er bindene. Schartum skriver om beslutningssystemer i offentlig forvaltning. Det er ikke akkurat det samme som straffesakssystemene, men tankene Schartum har rundt beslutningssystemene er i høyeste grad relevante også for straffesakssystemene. I

automatiserte beslutningssystemer fastlegges kodene. Som Luhman sier, er kodene bindene. Schartum skriver at den forståelsen som innprintes i datasystemene er den som vedtas som den riktige forståelsen. Et eksempel er en lovtekst. De kan være vage og vanskelige å tolke. Når de nedfelles i et datasystem blir de tillagt en mening, og tolkningsrommet blir til en viss grad borte (Schartum: 2002: 125). Derfor er det viktig med kontroll av kodene til systemene. Noen ganger nedfelles kodenenes betydninger i egne dokumenter, andre ganger er det kun utviklet såkalte kravspesifikasjoner. Uansett format er dette dokumenter som Schartum mener må utsettes for kontroll for å sikre kvaliteten på resultatet som kodene er grunnlag for (Schartum, 2002: 128). I tilfeller hvor det kun er enkeltpersoner som har inngående kunnskap om systemene, samsvarer ikke det med gode rettssikkerhetsidealer. Schartum mener at det heller ikke kan aksepteres som en kostnad som må betales for å oppnå mer av noe annet. God dokumentasjon av rettslige systemavgjørelser gjør det enkelt for tilsynsmyndigheter og eventuelle andre å forstå regelanvendelsen (Schartum, 2002: 129).

Chan (2001/2003) drar en parallell mellom Bourdieus teori om kapital og habitus, og teknologi. Teknologi gir mulighet for kunnskap, gjenkjenning, samarbeid, kommunikasjon, informasjonsdeling, handling og forebygging. Dette kan sees som en type makt, eller en kapital som gir makt innen et visst område. Teknisk ekspertise har blitt en kulturell kapital som henger høyt. Innføringen av IKT-systemer har gitt mye som kanskje glemmes i hverdagen. Chan viser at ved å sammenligne seg med noen som ikke har tilgangen til de samme teknologiske løsningene, kommer det frem at forskjellene er store (Chan, 2001: 149). Den teknologiske utviklingen skjer så raskt at det er fort gjort å henge etter. Uansett har politiet mye teknologisk kapital sammenlignet med de som ikke har datasystemer. Chan (2001) har undersøkt hvordan IKT påvirker politiets praksis i Australia. Hun skriver at IKT har gitt et skifte i habitus fordi IKT blant annet har gjort politiets prosedyrer mer gjennomsiktig, mer åpne og lettere tilgjengelig for publikum. Publikum ser dette som en indikator på bra politiarbeid (Chan, 2001: 156). Hvordan teknologien påvirker politiet avhenger av de tekniske mulighetene, men også av den innarbeidede kulturen, verdiene, styringen og rutinene (Chan, 2001: 147). Chan kaller dette samspillet for «The technological game».

Å ha kunnskap om straffesakssystemene kan altså være en form for kulturell kapital. For politiet er det av stor verdi å ha gode dataferdigheter, dermed innehar de som er flinke med dataprogrammene en kulturell kapital innenfor politikulturen generelt. De som ikke har de samme ferdighetene bruker til gjengjeld lang tid på å utføre oppgaver på data, og de bidrar ikke til effektivisering (Chan, 2003: 664-665). Med bakgrunn i dette er det lett å forstå at datasystemer som er lite brukervennlige, som straffesakssystemene, gjør det enda verre for de brukerne som har lite datakunnskap, og effektiviseringen svekkes ytterligere. Teknologi kan være en maktkapital, men det må henge sammen med tillit. Skirbekk ser det å få tillit av andre som en sosial kapital (Skirbekk, 2012: 13). Dermed kan god teknologi bidra til flere typer kapital.

Sosiale, kulturelle og politiske forhold spiller ofte inn i tillegg til selve teknologien. Selve teknologien handler om hvor godt eller dårlig systemet er (Chan, 2001: 144). De kulturelle faktorene handler om hvordan teknologien brukes, mottas og forstås av de som bruker den (Chan, 2001: 145). Den politiske dimensjonen handler om at det ligger makt i de teknologiske løsningene og for de som bruker dem (Chan, 2001: 146).

6.5 Kultur som forklaring

Kultur et begrep som favner mye, kan ilegges ulik betydning og det finnes mange definisjoner av begrepet. Opprinnelig betydde kultur *dyrking* ifølge Store norske leksikon, men i dag omfatter begrepet betraktelig mer. En definisjon er følgende:

Det generelle kulturbegrepet omfatter tanke-, kommunikasjons- og atferdsmønstre på alle felter av samfunnslivet, uavhengig av om det finnes noen spesialisert kultursektor eller ikke. Ofte tenkes slike mønstre å overlape ulike felt og sektorer på en slik måte at kulturen fremstår som sammenhengende og helhetlig. Forestillingen om slike sammenhengende helheter gjør det også mulig å snakke om kulturer i flertall. Da tenkes det ofte at hver kultur tilsvarende ett folk eller samfunn (norsk kultur, samisk kultur osv.), men begrepet kan også brukes om enheter på ulike nivåer (for eksempel vestlandsk kultur, norsk kultur, europeisk kultur osv.). Ulikt det sektororienterte kulturbegrepet impliserer det generelle kulturbegrepet ikke verdibaserte graderinger, men man kan likevel tenke seg at helhetene omfavner underordnede varianter (Store norske leksikon).

Subkultur er en type kultur som gjerne knyttes til spesielle miljøer. Politikk, økonomi og samfunnets organisering er også aspekter ved kultur, selv om kanskje ikke alle er enig i det. Ettersom kulturbegrepet favner så mye som det gjør, synes det nødvendig å diskutere også i

denne sammenheng. Det kan derfor være hensiktsmessig å koke begrepet ned til *yrkeskultur*. En yrkeskultur oppstår blant de ansatte i en organisasjon som et verdigrunnlag de ansatte opptrer etter. Verdier formes etter organisasjonen og arbeidsoppgavene til de ansatte. Patruljerende politi og analytikerne er eksempler på interne grupper hvor det kan oppstå ulike kulturer innen samme yrke fordi de har ulike oppgaver (Chan, 2003: 674). Slik jeg forstår Foster (2003) handler yrkeskultur om både væremåte og tenkemåte, og det er tankegangen som styrer handlemåten. Hvis kultur forstås som en tenkemåte kan en påstå at politiet har en kultur for å tenke at «det går som regel bra». Dette fordi de er hendelsesstyrte, og fordi det som regel går bra. Hvis det så skjer noe som viser at det ikke går bra, blir et hendelsesstyrt politi stående litt rådvillt. Forutsigbarhet er et viktig element i politiets arbeid, noe som kan være vanskelig å oppnå fordi de opptrer i uforutsigbare miljøer (Foster, 2003: 197).

Det er lett å forstå at kulturforklaringer er nyttige. Det er imidlertid vanskelig å fremstille i detalj når og hvordan kulturforklaringer er relevante, og hvordan utfallet av kulturforklaringer kan bli (Garland 1990: 209). I og med at kultur er et begrep som rommer så mye som det gjør, blir det for lett å bruke det som forklaring på hvordan sosiale mønstre dannes. Av samme grunn kan det heller ikke avskrives. Jeg tror at kulturforklaringer har mye å bidra med og er viktig for å forstå de fleste sider av den sosiale virkelighet, men det er ikke legitimt som en enestående forklaring på hvordan politiet har havnet i en situasjon med utdaterte straffesakssystemer. Kultur er en faktor som kan tenkes å være i samspill med andre faktorer som for eksempel organisering og ledelse. Foster (2003: 196) skriver at det ikke er én politikultur, men flere. Finstad argumenterer for det hun kaller et variert kollegafellesskap. Hun skriver at politiet etterstreber å skape et variert politi både geografisk, etnisk og kjønnsmessig, men at det samtidig er visse personlige egenskaper som vektlegges under opptak til politihøgskolen (Finstad, 2013: 235-236). Samtidig som en politikultur har mange fellestrekk, er det variasjoner innenfor dette. Som jeg har nevnt tidligere, kan det oppstå ulike praksis for å utføre samme arbeidsprosess i forskjellige distrikter. Det kan gjøre at det skapes ulike kulturer i det enkelte distrikt. Ulike kulturer kan virke negativt på samarbeidet mellom distriktene, ledelsen blir utøvet forskjellig og resultatet avhenger ikke lenger av målet, men av kulturen i det enkelte distrikt (Politianalysen, 2013: 155). Det er sannsynlig at kultur er en faktor som har påvirket arbeidsprosessene til å bli ulike, og dermed når ikke etaten sine felles mål som for eksempel effektiv kriminalitetsbekjempelse. Samtidig har etaten hatt lite fokus på

ledelse. Svak ledelse og ulike arbeidsprosesser gjør at publikum blir usikre på hva de kan forvente av politiet, og deres tillit til politiet kan dermed bli svekket.

Et variert kollegafellesskap er helt normalt, men den type ukultur som en snokekultur er bør elimineres. En styrket ledelse kan ta kontroll over snokekulturen og fjerne den slik at tilliten fra publikum kan bedres. Foster (2003: 219) drøfter om det er mulig å forandre en politikultur. Hun skriver at operativt politi kan være vanskelig å kontrollere fordi de operer utenfor politihuset. En snokekultur kan være lettere å kontrollere fordi snokingen foregår inne. Det blir enda lettere å kontrollere når systemene får funksjoner for logging, slik politiregisterloven krever. Foster skriver at så lenge de ansatte er mottakelige for forandring av kulturen så er det mulig. Hun trekker frem et eksempel Janet Chan forsket på ved New South Wales politikammer. Der foregikk det korrupsjon, men en sterk ledelse gjorde det helt klart at det ikke ble tolerert, og problemet tok slutt (Foster, 2003: 219-220).

Chan har et godt poeng som er relevant for denne oppgaven, når hun skriver at kulturelle forandringer foregår over tid, men den teknologiske utviklingen skjer i et så hurtig tempo at det er ikke rom for at nye kulturer får satt seg. Det er også vanskelig å forutse hva som vil være mulig å gjøre med teknologien i fremtiden. Dermed er det også vanskelig å møte endringene (Chan, 2003: 668).

6.6 Fra isolerte til standardiserte arbeidsprosesser gjennom strategiske virkemidler

Brukeren mener at det ikke vil hjelpe med nye systemer fordi det er menneskene som feiler. Derfor bør det være manuell kontroll av alt som registreres inn, ifølge brukeren. Situasjonen kan likevel bli bedre, men mange av feilene vil aldri forsvinne helt. Ett system med ett sett personinformasjon vil gjøre det enklere og være ressursbesparende. I kapittel 4 skrev jeg at brukeren mener det må gjøres noe med kvalitetskontrollen og rutiner. Rutiner bør være så tydelige og enkle som mulig. De bør læres gjennom opplæring som også presenterer regelverket, og det bør være intern kontroll som avdekker eventuelle feil (Et ansvarlig politi, 2009: 161). Når noe går galt synliggjøres kunnskapsmangler, derfor bør politiet ha kunnskap om risiko. Opplæring, kunnskapssøking, oppfølging, og gjennomgang av regelverk må skje

jevnlig for å sikre kontinuerlig oppdaterte rutiner og minimalisere risiko (Et ansvarlig politi, 2009: 162).

Som jeg skrev i delkapittel 6.1 mener Vaughan (1999) at avvik i organisasjoner skapes gjennom manglende samsvar i rutiner. Manglende samsvar i rutineene kan føre til feiltakelser, dårlig forvaltning og katastrofer. Ifølge Vaughan, er det de samme prosessene som skaper feiltakelser, dårlig forvaltning og katastrofer som skaper god forvaltning. Det er derfor vanskelig å vite når grensen for god og dårlig forvaltning er krysset (Vaughan, 1999: 292). Det sentrale problemet er, ifølge Vaughan, hvordan risiko og usikkerhet konstrueres. Den sosiale konteksten for konstruksjonen er sentral fordi konstruksjonen varierer med den sosiale lokaliseringen konstruksjonen foregår i (Vaughan, 1999: 295). Når organisasjoner tilegner seg mørke sider, er det en form for egen vranglære. Tilbakemeldingsprosesser som ikke fungerer tilfredsstillende er et eksempel på slik vranglære. Hvis det ikke gis tilbakemeldinger, eller hvis tilbakemeldingene er upresise, så oppdages ikke feil. De vil derfor heller ikke bli rettet opp i (Vaughan, 1999: 278). Av og til aksepteres mindre feil og mangler for å nå tidsfrister og holde seg til gitte ressurser. Hver gang feil og mangler aksepteres tøyges grensene for hva som aksepteres neste gang.

I Politianalysen anbefales det å utvikle standardiserte arbeidsprosesser, og at IKT må brukes likt av alle (Politianalysen, 2013: 45). Straffesakseksperter sa at politiet må organisere arbeidet sitt bedre, og ha konkrete IKT-strategier for å få bedre måloppnåelse. I Rapport fra 22. juli-kommisjonen (2012: 455) står det at kommisjonen har observert at Politidirektoratet og Justisdepartementet er enig om at dagens IKT-situasjon er bedrøvelig. Sentrale ledere vet altså at situasjonen er alvorlig. Når det er uttalt bør det kunne forventes at det settes i gang tiltak før, og i tillegg til, MERVERDIprogrammet. Videre sa straffesakseksperter at det er gjort masse i POD, politisjefmøtene og i PDMT for å fokusere på planer. Dette bekreftes i Politianalysen (2013: 193) hvor det står at Politidirektoratet nå har utarbeidet en IKT-strategi, og at det jobbes med å heve kompetanse, bedre styringen og endre organiseringen. Som straffesakseksperter sa, er politiet vant til å sitte på hver sin tue og pusle med sitt. Det dannes stadig småprosjekter som skal utbedre og utvikle enkelte områder, men sammenhengen mellom områdene blir ikke sett. Det blir heller ikke sett utover landegrensene for å lære. De isolerte arbeidsprosessene påpekes også i en masteroppgave fra Politihøgskolen:

Det er liten tradisjon for å arbeide på tvers av avdelinger. Man jobber isolert med oppgaver uten å se disse i sammenheng. Det kan virke som målet blir å finne en løsning på situasjonen man står i uten at informasjonen fra denne blir videreført for å forebygge fremtidige kriminelle handlinger (Tinholt, 2013: 29).

Det er viktig å se ting i sammenheng, men det er også en risiko knyttet til å tenke for stort. Prosjekter kan bli så omfattende at de ikke kan gjennomføres. Derfor er det viktig å samle inn kompetanse og kunnskap om aktuelt område. Hvis politiet skal finne opp kruttet på nytt for hvert område de ser på, vil de bruke unødvendig mye tid.

Torill Iversen har skrevet en masteroppgave om politiets IKT-systemer. Hun konkluderer med at politiet er umoderne vedrørende IKT, det er mangel på IKT-styring og lav kompetanse på alle nivåer (Iversen, 2012: ii). Iversen skriver at gjennom mer opplæring og kunnskap kunne politiet hatt et forbedringspotensial innen de løsninger som allerede foreligger. Derfor sier hun at det må skje en holdnings- og modenhetsendring i etaten hvis en skal ha nytte av IKT-oppussingen. Også straffesakseksperten fortalte om denne modenheten. Regjeringen har ikke ønsket å bevilge penger til IKT-utvikling tidligere fordi de har ment at etaten ikke er moden nok. I dette ligger at politiet ikke ble ansett som modne til å forvalte midlene riktig i mangel av strategiske planer og virkemidler. Ifølge straffesakseksperten baserte regjeringen dette på, blant annet, Accenture (2010) sin rapport. Denne modenheten har imidlertid utviklet seg og politiet jobber fortsatt med modningsprosessen.

Gundhus (2006: 469) skriver at politiet ikke har en kultur for bruk av IKT som et kunnskapsverktøy. Avhandlingene til Iversen og Gundhus har flere likhetstrekk. Selv om vi har studert ulike sider ved IKT i politiet, mener jeg at vi har funnet noe av det samme. Det er ingen tvil om at IKT-systemene er umoderne, og en av grunnene til det er at det har vært for dårlig IKT-styring og lite innovativ tenkning. I tillegg er det lav kompetanse om det som finnes. Det betyr at dagens systemer kunne vært utnyttet bedre.

I Politianalysen forklares strategisk kompetansestyring slik:

Strategisk kompetansestyring er et verktøy og en arbeidsmetode for å sikre at virksomheten har nødvendig kompetanse for å nå sine mål, både på kort og lang sikt. Dette innebærer å kartlegge behov, utvikle planer og iverksette tiltak for å fylle gapene mellom eksisterende kompetanse og (fremtidig) kompetansebehov (Politianalysen, 2013: 209).

Videre fremkommer det at politiet kunne vært bedre på strategisk kompetansestyring. Det er for lite helhetlig og systematisk tenkning rundt utvikling. Selv om det er planer er det lite som faktisk iverksettes, og det følges heller ikke opp i etterkant (Politianalysen, 2013: 206).

Effektiv etterforskning og straffeforfølgning er to av kriteriene utvalget setter for hvor godt politiet kan løse sine kjerneoppgaver (Politianalysen, 2013: 22). For å oppnå effektivitet er IKT sentralt. Enkle søk, enkelt å registrere, enkelt å hente ut og dele informasjon samt standardiserte rutiner er en forutsetning for effektivitet (Politianalysen, 2013: 23). IKT-verktøyene skal være strategiske virkemidler som politiet benytter for å oppnå effektiv oppgaveløsning. I kapittel 4 viste jeg at det er utfordringer knyttet til straffesakssystemene som strategiske virkemidler for effektiv oppgaveløsning. I Politianalysen (2013: 203) anbefales det at Politidirektoratet snarlig ferdigstiller arbeidet med å kartlegge systemer, mangler og behov slik at de kan lage gode strategier for IKT og effektivisering. Som en del av dette arbeidet tenker jeg at risikovurderinger bør utføres. Det vil gi et bedre grunnlag for å vurdere behovene og det blir tydeligere hva som må prioriteres. Til tross for at det er flere risikoelementer og at risikoene kan få store konsekvenser, er det ingen rutine for å foreta risikovurderinger i dag. Å ha kunnskap om risikoene som foreligger er helt sentralt for å kunne forebygge og håndtere alvorlige hendelser. Risikoanalyser er et godt grunnlagsmateriale for å sette inn virkningsfulle tiltak. Slike analyser dreier seg om å tilegne seg kunnskap over tid ved å se på sannsynligheten for en forekomst og konsekvensene av ulike utfall. I tillegg må det tas høyde for uforutsette momenter (Rapport fra 22. juli-kommisjonen, 2012: 451). Uten risikovurderinger har ikke politiet egnet informasjon til å tilrettelegge straffesakssystemene slik at de fungerer som gode verktøy for effektiv oppgaveløsning. Risikostyring er tiltak og aktiviteter som settes i gang for å styre risiko for å unngå tap. Det dreier seg om planlegging, identifisering, analysering og håndtering av risiko. Ulike analysemetoder er utviklet spesielt med tanke på risiko i informasjonssystemer.

Et eksempel på et enkelt skjema for risikovurdering vises under. En risikoanalyse ville for eksempel kunne anslå hvor stor sannsynlighet det er for at en person blir dømt til for lav straff på grunn av feil eller mangler i politiets registre og hvilke konsekvenser det kunne få. Ligger krysspunktet mellom konsekvens og sannsynlighet i en rød rute, betyr det at denne risikoen bør vurderes som uakseptabel og må gjøres noe med.

KONSEKVENNS	Svært alvorlig	E1	E2	E3	E4	E5
	Alvorlig	D1	D2	D3	D4	D5
	Moderat	C1	C2	C3	C4	C5
	Liten	B1	B2	B3	B4	B5
	Svært liten	A1	A2	A3	A4	A5
		Svært liten	Liten	Middels	Stor	Svært stor
		SANNSYNLIGHET				

Prinsipp over akseptkriterium. Forklaring av fargene som er brukt i risikomatriksen.

Farge	Beskrivelse
Rød	Uakseptabel risiko. Tiltak skal gjennomføres for å redusere risikoen.
Gul	Vurderingsområde. Tiltak skal vurderes.
Grønn	Akseptabel risiko. Tiltak kan vurderes ut fra andre hensyn.

Dette skjemaet er helt enkelt, men det finnes svært avanserte metoder for risikoanalyse. Som jeg skrev over, dreier risikoanalyser seg om å tilegne seg kunnskap over tid ved å se på sannsynligheten for en forekomst og konsekvensene av ulike utfall. Jeg har ikke grunnlagsmateriale til å utføre en slik analyse, men det har politiet. Jeg kan likevel prøve meg på et eksempel. I kapittel 4.2 skrev jeg at det er risiko for at stormaskinen til Strasak kan kollapse. Systemet begynner å bli fullt, og det er få personer som kan håndtere maskinen. Om den kolliderer kan det få store konsekvenser. Kanskje alvorlig eller svært alvorlig er passende klassifisering i skjemaet over. Ettersom maskinen ikke har knelt allerede, er kanskje ikke sannsynligheten for at det skjer så stor. På en annen side blir sannsynligheten bare større jo lenger tid det går og jo mer fullt systemet blir. Liten eller middels er muligens korrekt plassering i skjemaet. Dermed blir krysspunktet i rute D2, D3, E2 eller E3. Tre av rutene er røde og at systemet kolliderer bør derfor vurderes som uakseptabel risiko.

Faren med risikovurderinger er klassifiseringen. Ting blir tatt ut av sammenheng, satt inn i standardiserte skjemaer og får tildelt en verdi som skal avgjøre noe. Schartum skriver at skjemautfylling er en slags bakgrunn for risikoanalyser. Utfylling av skjemaer er gjort i lang tid, det er ikke noe som kom med IKT. IKT-innføringen har imidlertid gjort at informasjonen er lettere tilgjengelig og bedre egnet til analyser. Problemet er at skjematerte svar er svar som stripes for skjønn og tolkningsrom. Vurderingen er allerede begått idet svaralternativet ble lagt inn i systemet. Derfor foreslår Schartum at automatiserte rutiner utformes slik at det

er mulig å være fleksibel. Systemene må kunne forandres etter at man gjør erfaringer. I tillegg mener Schartum at utformingen av beslutningssystemer bør være gjenstand for offentlig debatt (Schartum, 2002: 135).

Jeg vil trekke frem et par eksempler på risikovurderinger hentet fra kriminologisk litteratur. Dette gjør jeg for å få frem den vide spredningen risikoanalyser kan benyttes i, og for å vise at risikovurderinger ikke bare er positivt. Det risikovurderes på skoler, på byggeplasser og i fengsler. Som eksempel kan jeg trekke frem Shearing & Stenning (1998: 40-45) som skriver om risikovurdering i en fornøyelsespark. De viser hvordan Disney World bruker risikovurderinger for å skape orden gjennom instruksjoner, systemer og overvåkning. Målet er å håndtere store folkemengder på en effektiv måte. Det er standarder for håndtering av avvik. For eksempel blir det å gå barbert ikke tolerert selv om man har gnagsår. Hvis ikke instruksjonene følges, resulterer det i utkastelse. På den måten trenes publikum opp til å følge instruksjonene, uten at Disney World kjenner publikumsindividene. Shearing & Stenning (1998) mener Disney World ser dette er effektivt fordi publikum ledes til å samarbeide, da det er mer behagelig å følge ordre enn å motsi ordre.

Et annet eksempel er Hannah-Moffat (1999) som ser på risikovurderinger av kvinnelige fanger i Canada. Hannah-Moffat sier at måten de behandler kvinnene på i canadiske fengsler har endret seg. Måten kvinnene behandles på skiller seg fra måten fengslene responderer mot menn. Fengslene mener det er forskjeller mellom kjønnene som må tas hensyn til ved risikovurdering og straff. Kvinners behov ses opp imot risiko. Der det er utilfredstilte behov, er det potensielle risikoer. Hannah-Moffat mener at denne tankegangen er uheldig og må modifiseres. Jeg tror likevel det er noe i denne tankegangen. Politiet har behov for at straffesakssystemene fungerer som gode verktøy for deres oppgaveløsning. De områdene hvor det kan oppstå risiko er områder hvor politiet ikke får oppfylt sitt effektivitetsbehov. Videre skriver Hannah-Moffat at fangene får et nummer mellom en og fem etter hvilken risikogruppe de tilhører. Det får videre betydning for både privilegier og oppsyn (Hannah-Moffat, 1999: 76). Det forventes også at fangene styrer seg selv til en viss grad, ved å unngå situasjoner, adferd og andre innsatte som anses som risikable. På den måten behandles kvinnene, paradoksalt nok, som om de er frie, rasjonelle og ansvarlige individer. Hvordan man velger å handle er imidlertid ikke alltid likt i og utenfor fangenskap (Hannah-Moffat: 79). Fangene vet at de risikovurderes, kategoriseres og settes i båser. Derfor lærer de seg hva de bør svare på spørsmål, og hvordan de bør oppføre seg for å bli ansett som lavrisikofanger. Hannah-Moffat

(1999: 88-89) konkluderer med at risikotankegangen er en del av et større neo-liberalistisk styringsprogram som ønsker å disiplinere og ansvarliggjøre kvinnelige lovbrøyttere. Videre mener hun at dette er lite effektivt, lite objektivt og at moralen ikke er byttet ut med et forsikringsmål. Som hun skrev, kan fangene påvirke hvilken bås de settes i. Det kan ikke et system som risikovurderes, men de som risikovurderer bestemmer hvor mye risiko som skal aksepteres. Det betyr at politiet kan påvirke risikovurderingen av et system annerledes enn hvordan et kontrollorgan eller en annen utenforstående ville gjort. Offentlige analyser vil kunne minske den utfordringen.

6.7 Merverdi for fremtidens politi

Accenture skrev i 2010 at PDMT har kortsiktige planer, og kun leverer der det brenner. Manglende samsvar mellom tildelte midler og omfanget på oppgavene som skal løses er en av grunnene til dette (Accenture-rapport, 2010: 2). Accenture anbefalte å foreta kompetanseheving og gjennomgå metodikk og arbeidsprosesser for å sikre bedre robusthet i moderniseringsprosessen av politiets IKT (Accenture-rapport, 2010: 3). Det arbeidet er blant annet satt i gang gjennom MERVERDI-programmet.

Straffesakseksperten fortalte at prosjekt 1, som er den første lanseringen, kommer i 2017. Da skal alle gamle data være konvertert, og det skal være et helt nytt saksbehandlingssystem som gir nye og ressursbesparende arbeidsprosesser. Informanten fortalte at det vil bespares minst 340 årsverk og at bedre informasjonsflyt er ett av de store målene. «Vi har diskutert informasjonsflyten og avgrensninger som vi må regulere etter politiregisterloven, men vi skal få bedre tilgang til informasjon som gjør at politiet kan jobbe på en bedre og mer effektiv måte.» Videre sa informanten:

Når politiet får informasjon, når vi konverterer sakene, får vi fem millioner saker i systemet. Det er sykt mange dokumenter fra BL som vi vil kunne søke i, og vi kan søke i mer dynamisk informasjon. Vi har ingenting nå i forhold til det vi kommer til å få. Hadde vi skjont det da vi hadde NYSS⁶ hadde publikum hatt det bedre nå.

⁶ NYSS står for nye straffesakssystemer og var et av prosjektene som la veien for MERVERDI-programmet.

At plattformen fungerer og at internett er tilgjengelig er ikke MERVERDIprogrammet sin oppgave, det ser programmet som en forutsetting. Det ansvaret ligger hos PDMT.

Systemspesialisten fortalte at det jobbes med og snart vil være på plass. Plattformen og internett ble forbedret og ferdigstilt underveis i dette prosjektet. MERVERDIprogrammet ønsker å effektivisere, tilgjengeliggjøre og skape et fleksibelt politi. Straffesakseksperter fortalte at navnet på programmet henger sammen med at arbeidsprosesser vil endres. Det vil gi merverdi av kunnskap, ressurser og teknologi. Straffesakseksperter er helt sikker på at bedre systemer vil bidra til høyere oppklaringsprosent og mer forebygging. Juristen er mer tvilende til hvor stor virkning nye systemer vil gi.

Ifølge straffesakseksperter, har ikke sammenhenger mellom elementer som hører sammen blitt sett under tidligere IKT-utviklingsarbeid. Politiet har jobbet ut ifra at systemene ikke snakker sammen. Med det menes at straffesakssystemene ikke har blitt sett som systemer i samme kjede, men som isolerte verktøy. MERVERDIprogrammet fokuserer derimot på arbeidsprosesser og hvordan et samlet straffesakssystem kan gjøre oppgaveløsningen mer effektiv. Politiet får altså gevinster ved å se hele bildet i sammenheng.

MERVERDIprogrammet er det største tiltaket som er satt i gang for å bedre IKT-situasjonen til politiet. Tiltaket er historisk og vil berøre alle ansatte i politiet. Situasjonen vil bli en helt annen for både politiet og publikum hvis målene til programmet nås. Skal vi tro på visjonene til MERVERDIprogrammet, er det verdt ventetiden. Publikum får også merke endringer ved at det blir bedre tjenester og enklere dialog gjennom større grad av digital samhandling. Forhåpentligvis vil også tiden som frigjøres til politiets kjerneoppgaver komme publikum til gode gjennom høyere oppklaringsprosent, mer tilgjengelig politi og mer forebygging.

Likevel, det er syv år til planlagt slutføring av programmet. All informasjon som finnes i dagens løsninger må konverteres over i nye systemer, og det må ryddes i gamle systemer for at informasjonen som konverteres skal være korrekt. Da tenker jeg først og fremst på at de registrertes identitet er korrekt og samlet på en og samme på person. Juristen påpeker at det er en risiko for at informasjon blir liggende på feil person for alltid. I tillegg må informasjon og personer som skulle vært slettet faktisk slettes. Så må nye systemer testes, feil må rettes, ny testing osv. Hartvigsen skriver at når informasjonssystemer utvikles, mangler det ofte nødvendige risikogjennomganger underveis:

Det forutsettes rask produksjon, hurtige endringer og mye dynamikk i utviklingen. Verifikasjoner, testing og risikoanalyser forsinker produksjonshastigheten av programkode og blir derfor ofte noe som

gjøres etter at kode er produsert. Det er en fare for at risikogjennomganger blir en kandidat som salderingspost når prosjektmidlene blir mindre i slutten av et utviklingsprosjekt. Det er derfor viktige at kriterier for risikogjennomganger med fokus på MTO, er et krav i utviklingsplaner og at tilstrekkelig med ressurser blir avsatt til dette (Hartvigsen, 2013: 73).

I Politianalysen (2013: 204) står det at dagens IKT-situasjon krever strakstiltak utover MERVERDIprogrammet. Northrop mfl. (1995) sine studier dokumenterer at lav brukervennlighet og tekniske problemer påvirker organisasjonen negativt. Når nye systemer implementeres må overgangen styres av en sterk ledelse og designet må være bra for at det skal bli en suksess (Chan, 2003: 670-671).

6.8 Lærdom fra andre etater og andre land

Altinn er et nettsted for innlevering av offentlige skjemaer som 17 offentlige etater samarbeider om (Lintvedt, 2007: 51). I 1997 begynte arbeidet med utviklingen av det som skulle være en løsning for elektronisk overlevering av opplysninger til Skattedirektoratet, Brønnøysundregistrene og Statistisk sentralbyrå. I 1999 gikk løsningen i pilotproduksjon. Det ble snart klart at det var mulig å få til bedre løsninger, og i 2001 ble det lagt frem en rapport om dette. I 2004 gikk Altinn i produksjon, og etter det er det kontinuerlig gjort forbedringer og endringer (Lintvedt, 2007: 52).

Altinn er svært ulikt straffesakssystemene, men det er likevel mulig å gjøre noen sammenligninger. Det er nemlig lagt ned et utviklingsarbeid som har ført til noe stort, med god kvalitet, i løpet av syv år. Nå har ikke jeg intervjuet noen fra skatteetaten eller satt meg spesielt godt inn i deres situasjon. Men i og med at IKT var lite utbredt i staten før på 80-tallet, mener jeg at situasjonen kan sammenlignes med politiets. Begge startet å utvikle egne systemer samtidig som den teknologiske utviklingen generelt skjøt fart. Nytt lovverk som skal ivareta god forvaltning gjennom IKT har også kommet med krav underveis. Med dette utgangspunktet har Altinn kommet langt på syv år, mye lenger enn politiet. Accenture er leverandør av Altinn (Lintvedt, 2007: 53), og de skal også levere nye straffesakssystemer. Det er mange faktorer som spiller inn for mulighetene til å utvikle gode løsninger og jeg skal ikke trekke sammenligningen for langt. Altinn er ikke hundre prosent optimalt, det er både mangler

og begrensninger i løsningen, men poenget mitt er at det er mulig. Kanskje kan politiet lære noe av skatteetaten og de andre som er involvert i Altinn. I en Analyse om IKT-styringen i politi- og lensmannsetaten (2013) har Politidirektoratet sett på IKT-styringen i andre etater og land. Lærdommen de trekker ut etter en felles vurdering er denne:

Gjennomgående for virksomhetene er at både premissgiver og leverandør er representert i toppledelsen. Det er i hovedsak ulike fagavdelinger som har ansvar for premissgiver- og leverandørrollen. Det synes å være etablert gode prosesser for porteføljestyling og virksomhetsstyring, og at virksomhetene har trukket leverandørfunksjonen nærmere til seg enn hva tilfellet er i politiet (Analyse av IKT-styringen i politi- og lensmannsetaten, 2013: 12).

Systemspesialisten gir et eksempel på at vi henger etter resten av Europa: «Nå kom jo nettbrettet, og det er en kjempeutvikling. Follo har vært pilot, og de er storfornøyde, men vi henger jo etter. De har hatt det i resten av Europa, til og med i østblokklandene. Jeg vet ikke hvor sikker løsning de har, men det kom sent her i alle fall.»

Ericson og Haggerty (1997) skriver om situasjonen i Canada. Det kan synes som om feltet de har undersøkt er annerledes enn forholdene i Norge. De hevder at canadisk politi har vært ledende innen datasystemer. Innen enkelte områder har norsk politi også hatt moderne og god teknologi. Likevel peker offentlige rapporter på store mangler og umoderne IKT som preger etaten. Ericson og Haggerty (1997: 389) skriver at canadisk politi hele tiden etterstreber det nyeste på markedet. Boka deres, *Policing the risk society*, er fra 1997. Forfatterne skriver at da holdt canadisk politi på å utvikle mobile enheter for at politiet kunne være mer ute og mindre på kontoret. Denne utviklingen samt nye systemer som skulle anskaffes, hadde en antatt kostnad på rundt 300 millioner dollar. Det er altså 17 år siden Canada var der Norge er nå. Grunnen til at de vil være ledende innen teknologiske løsninger i Canada er, ifølge Ericson og Haggerty, at det vil gi dem mer kunnskap om risiko. En systemspesialist Ericson og Haggerty intervjuet mente at det å være ledende innen datateknologi var viktig for å vise vilje til reform og fremskritt (Ericson og Haggerty, 1997: 390).

7. Avslutning

I denne oppgaven har jeg vurdert ulike risikoer knyttet til politiets straffesakssystemer. Jeg har vist hvilke mulige betydninger disse risikoene kan ha for politiet, de registrerte, publikum og forholdet mellom dem. Følgende punkter gir en kort oppsummering av de mest sentrale risikofaktorene jeg har lagt vekt på:

- Tekniske feil og svakheter som kan føre til driftsavbrudd eller kollaps
- Lav brukervennlighet som kan føre til ulik registreringspraksis, feilregistrert personinformasjon, feil eller mangler i straffeattester og uriktige straffer
- Manglende funksjoner for logging og sporing som gjør det vanskelig å oppdage om det snokes i systemene
- Manglende muligheter for å implementere nytt lovverk som har ført til at ny straffelov ikke kan tre i kraft
- Unødvendig tids- og ressursbruk som kan føre til svekket effektivitet

Til sammen kan situasjonen føre til at publikum ikke har tillit til politiet, men undersøkelsene jeg har vist til viser samtidig at publikums tillit til politiet er relativ høy. Jeg har også drøftet ulike årsaksforklaringer som politiets organisering, ledelse, makt og kultur. Innføring av tiltak innenfor organisasjonsutvikling, kunnskapsutvikling og risikostyring kan gi vesentlige forbedringer både ved videre bruk av dagens systemer og ved innføring av nye systemer når disse blir ferdigstilt.

Risikoene i straffesakssystemene kan påvirke politiets arbeidssituasjon i negativ retning, og politiet har ingen fordeler ved å fortsette å ha dagens straffesakssystemer kontra ved å innføre nye systemer. Likevel har de naturligvis mange fordeler ved å ha dagens systemer i motsetning til å ikke ha noen systemer i det hele tatt. Blant annet har Luhman (1993: 28) påpekt at det ikke finnes risikofri atferd eller absolutt trygghet fordi avgjørelser ikke kan unngås for å forhindre risiko. Ericson og Haggerty har også vist til at det ligger et paradoks i å få mer kunnskap om risiko. Ønsket om sikkerhet krever mer kunnskap om risikoer, samtidig som mer kunnskap om risiko, og arbeidet med å styre risikoer, avdekker stadig ny usikkerhet.

The yearning for security drives the insatiable quest for more and better knowledge of risk. However, in the search for inexhaustibly detailed and continuous risk management knowledge, each new form of knowledge and the measure of protection it makes visible gives rise to new knowledge about insecurities (Ericson og Haggerty, 1997: 85).

Luhman har påpekt det samme. Han mener at fremtiden er en risiko.

Rettsikkerheten er til dels svekket på enkelte områder grunnet svakhetene i systemene, men ikke i like stor grad som jeg antok i forkant av prosjektet, og den er mest svekket etter den klassiske forståelsen av begrepet. Straffesakssystemene i seg selv svekker ikke rettsikkerheten, men de bidrar heller ikke til å opprettholde sterk rettsikkerhet. Tall som er presentert i oppgaven viser at det er få såkalte råtne epler i politiet, og at det rettes opp i feil når det oppdages. De fleste har høy lojalitet ved bruk av systemene. Juristen påpekte at med et lovverk som åpner for å ta vare på flere opplysninger, hadde politiet hatt et bedre utgangspunkt for sitt forebyggende arbeid. Dette kunne bidratt til styrket rettsikkerhet. Politiet kunne sannsynligvis utført sine arbeidsoppgaver mer effektivt, og lovbrudd kunne vært forebygget hvis politiet kunne bruke tiden annerledes og informasjonen var lettere tilgjengelig. Ny straffelov som ikke kan tre i kraft påvirker publikum fordi det ikke kan reageres mot visse typer handlinger i henhold til det som forventes av publikum i dagens samfunn.

Oppgaven har vist at politiet har tillit fra publikum. Publikum deler altså ikke Flyghed og Hörnqvist sin tvil til om staten er tillit verdig. Flyghed og Hörnqvist (2003) hevder at staten gjør ting som tilsynelatende er trygghetskapende, men ikke nødvendigvis positivt for alle. Jeg har vist at det ikke er tilfelle for politiets bruk av straffesakssystemene. Det finnes få alternativer til å ha tillit til staten fordi makten ligger hos staten og borgerne må stole på den. Publikum tvinges til å ha tillit til politiet og politiet tvinges til å klare seg med de systemene som er fram til nye systemer lanseres. Selv om publikum har tillit til politiet, kunne tillitsnivået vært høyere. Mer åpenhet utad kan øke tilliten, men folk kan også bli skeptiske. Snokekulturen og de få ansatte som ønsker å snoke kan redusere publikums tillit. Med politiregisterloven og nye straffesakssystemer vil det bli vanskeligere å snoke og forhåpentligvis færre råtne epler.

Jeg har argumentert for at politiet bør benytte seg av systematiske risikoanalyser for å kartlegge risiko, synliggjøre behov, vise handling, dele kunnskap og skape tillit. Fraværet av risikoanalyser, viser en erfaringsbasert holdning eller tankegang om at "det går som regel bra". Denne erfaringsbaserte tankegangen er noe av utfordringen for politiet fordi de uttrykker at de arbeider kunnskapsbasert, men gjennomfører ikke det i praksis (Gundhus, 2006 og

Tinholt, 2013). Tradisjonelt sett har politiet arbeidet etter henvendelser fra publikum, og derfor vært hendelsesstyrt og erfaringsbasert (Gundhus, 2006). Det har imidlertid skjedd et skifte. Risikosamfunnet har ført til endrede arbeidsmetoder i politiet ettersom kunnskap vektlegges i høyere grad enn før. Likevel er det fortsatt forskjell mellom hvor kunnskapsbasert politiet ønsker å være og hvor mye de faktisk er det. Å utføre risikoanalyser er et eksempel på hvordan politiet kan jobbe mer kunnskapsbasert. Kunnskap om risiko for å kontrollere det ukjente eller farlige er det som kjennetegner risikosamfunnet. En kunnskapsbasert risikoanalyse av straffesakssystemene må forholde seg til rettssikkerhetsprinsippene samt andre rettslige krav, og ikke bare finne praktiske løsninger for arbeidsoppgavene. Straffesaksekseperenten fokuserte mye på arbeidsprosesser og hvordan MERVERDIprogrammet vil endre politiets måte å jobbe på. Samtidig fortalte informanten at programmet har løpende kontakt med både lovavdelingen og datatilsynet for å sikre krav som stilles utenfra.

I oppgaven har jeg vist hvordan organisasjoner kan institusjonalisere avvik. Jeg har også drøftet begrepet akseptabel risiko. Mer kunnskap om risiko, bidrar til å finne mer risiko. Som Luhman poengterer, finnes det ikke risikofri atferd. Spørsmålet blir derfor hvor høy risiko som kan aksepteres, og ikke minst hva slags risiko som kan aksepteres. At den nye straffeloven ikke kan tre i kraft har blitt akseptert lenge, men diskuteres stadig. Jeg har brukt Punch og Vaughan for å vise hvordan organisasjoner kan utvikle såkalte mørke sider, systematisk produsere feil og normalisere avvik. Ved å leve med avvik over tid skyves grensene for hvor høyt risikonivå som aksepteres. Jeg tror det aldri vil bli akseptert for at den nye straffeloven ikke kan tre i kraft, men det kan være andre utfordringer med mindre konsekvenser som aksepteres. Ved å bruke datasystemer med flere risikofaktorer knyttet til seg over tid, vil lista for hvor høyt risikonivå som aksepteres hele tiden øke. Det som først anses som avvik og ugreit blir gjennom langvarig gjentakelse akseptert og gjort til noe normalt. Det som i utgangspunktet ikke kunne aksepteres blir etter hvert helt greit.

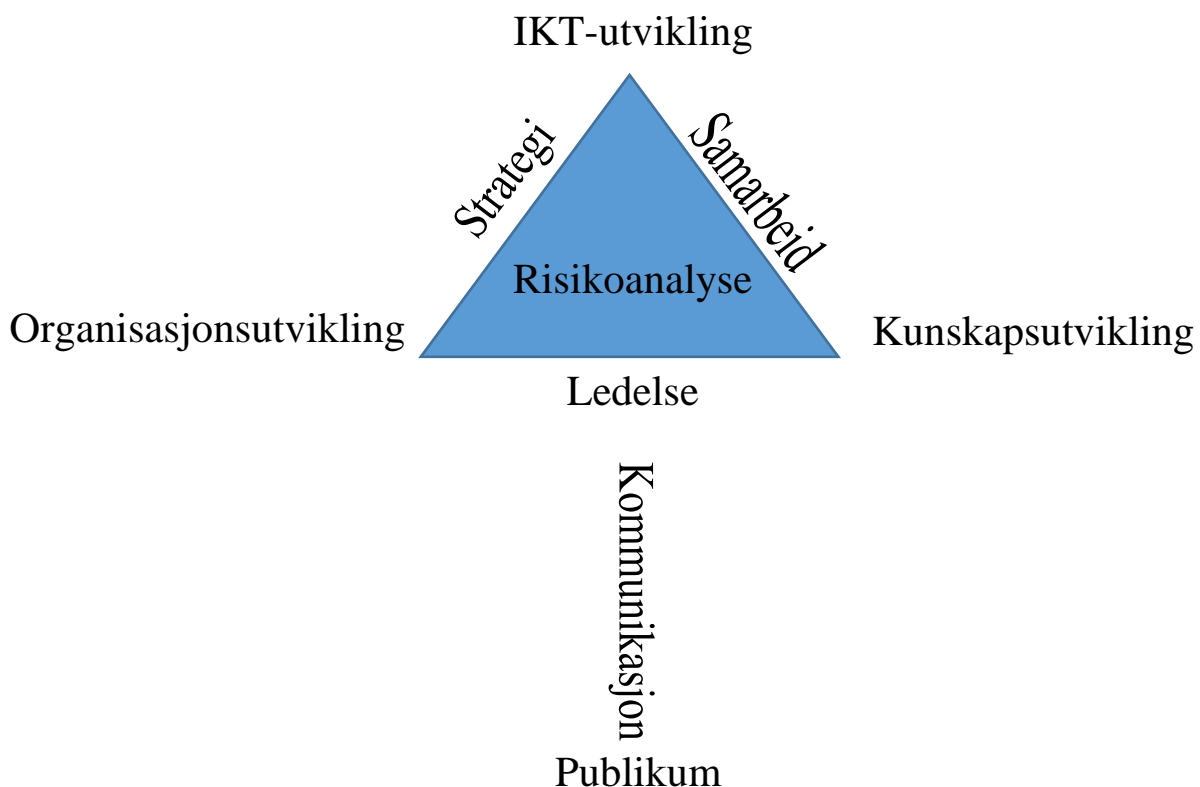
Ifølge Luhman er risiko og trygghet to aspekter vi hele tiden vurderer. Vi kan velge å gjøre noe risikabelt for å oppnå mer eller vi kan velge det trygge, uten å risikere noe, men heller ikke oppnå like mye (Luhman, 1993: 20). Slik jeg ser det i etterkant av intervjuene har ikke politiet noen alternativer. De tvinges til å ha risikable straffesakssystemer for å oppnå noe i

det hele tatt. Alternativet, frem til de nye systemene er på plass, vil være å falle tilbake til steinalderen, i alle fall papiralderen. Enn så lenge må politiet klare seg med de systemene som er, selv om de har risikoer knyttet til seg. Tvingen må likevel modifieres. Politiet har ikke vært flinke nok til å utvikle seg innen IKT, de har vært preget av for lite fokus på ledelse og de har ikke sett ting i sammenheng. En annen måte å se det på er at politiet velger å beholde datasystemer med betydelige svakheter. Dette for å oppnå mer av noe, nemlig mer kriminalitetsbekjempelse og trygghet for borgerne, enn det ville vært uten systemer i det hele tatt.

I en rapport fra Holte Consulting gis en oversikt over tiltak som er satt i gang, eller som skal settes i gang. Her står det at det har skjedd mer på IKT-fronten de siste to årene enn de ti foregående årene, men en del tiltak er forsinket (Rapport, 2013: 29). I rapporten presenteres en rekke anbefalinger hvor ett av dem er å etablere systematisk risiko- og kapabilitetsanalyser (Rapport, 2013: 30). Rapporten viser at det skjer mye innen IKT i politiet i disse dager, og det er et godt utgangspunkt for å snu trenden med svake IKT-systemer. MERVERDIprogrammet har noe av svaret på dagens utfordringer, men det løser ikke nye problemer i fremtiden. Det er heller ikke sikkert at nye straffesakssystemer vil bidra til høyere oppklaringsprosent og mer forebygging. Men forhåpentligvis vil politiet gjennom nye systemer få en mer tilrettelagt hverdag, og bedre forutsetning for å løse sine oppgaver på en effektiv måte. Det vil også bidra til at publikum trygges.

Situasjonen har blitt som den har blitt, blant annet fordi politiet ikke ser de aktuelle systemene som strategiske virkemidler til å løse sine arbeidsoppgaver. Ifølge straffesakseksperten ser departementet nå koblingen mellom politifag og IKT. Derfor blir denne koblingen prioritert i større grad enn tidligere. Dette er et ledelsesansvar. IKT-utviklingen må foregå i samspill med kontinuerlig organisasjonsutvikling. Det finnes ikke et enkelt svar på hvordan politiet kan snu trenden for IKT-utvikling for å unngå å havne i samme situasjon igjen. Informantene mener at det er den politiske styringen, hvor politikerne ikke har skjønnet hvor stort behovet for nye straffesakssystemer er, som er noe av forklaringen på dagens situasjon. Det blir for lett å skylde på politikerne, men en konklusjon kan være at virksomheten må drive kontinuerlig organisasjons- og IKT-utvikling som er i takt med den generelle teknologiske utviklingen i samfunnet. Samtidig må kunnskapsutvikling være en del av dette samspillet. Erfaringer er nyttige, men ikke tilstrekkelig når det oppstår nye og uvante situasjoner.

I likhet med Feeley og Simon (1998) mener Douglas og Lianos (2000) at verdier, ansvar og plikter er gamle verktøy for sosial kontroll. Farlighet er det nye, og samfunnet skaper en ond sirkel gjennom håndtering av farlighet: institusjonell aktivitet – kontroll – forutsigbarhet – sikkerhet – sårbarhet – farlighet – nye typer kontroll – ny institusjonell aktivitet. Under oppstarten av dette prosjektet lurte jeg på om jeg ville finne lignende typer sirkler som forklarer opprettholdelsen av dagens IKT-utviklingstrend. Jeg har funnet ut at politiet ser sine behov, vurderer ressursene sine og utvikler systemene deretter. IKT-utviklingen stopper av seg selv, fordi ressursene er mangelvare. Onde sirkler kan forklare hvorfor situasjonen har blitt som den har blitt. Så kan man kanskje se for seg en forklaringskjede som gjør at den onde sirkelen unngås. En forklaringskjede som både viser elementene for å oppnå effektiv oppgaveløsning, og hindrer at politiet blir umoderne i den teknologiske verden. Ut ifra drøftelsen i kapittel 6 kan en forklaringskjede se slik ut: Organisering – ledelse – IKT-verktøy – risikoanalyser – strategiske-planer – standardiserte rutiner. Hvis disse elementene er i kontinuerlig drift og sees i sammenheng, kan det være en kilde til mer effektiv måloppnåelse. Elementene må også være i kontinuerlig utvikling, og gjennom kommunikasjon til publikum kan tilliten økes ytterligere. Dette kan illustreres slik:



Etter hvert som dagens tilstand har blitt mer og mer avklart har tydeligheten av hvor omfattende det er å lage noe nytt vist seg. Behovet har blitt så stort at det er utfordrende å lage noe som tilfredsstillende alle krav, men det skjer masse positivt i politietaten om dagen og spenningen er stor rundt resultatene fra MERVERDIprogrammet.

Referanser

Accenture-rapport (2010): Evaluering av politiets data- og materieltjeneste.

Virksomhetsområde IKT. Oslo: Accenture

Adam, Barbara og Joost Van Loon (2000): «Introduction: Reposition risk; the challenge for social theory.» I: *The risk society and beyond. Critical issues for social theory*. Barbara

Adam, Ulrich Beck og Joost Van Loon (red.). London, Thousand Oaks, New Delhi: Sage Publications

Aftenposten (2009): «Politiet tar lærdom av «Lommemann»-saken.» URL:

<http://www.aftenposten.no/nyheter/iriks/article3435882.ece#.UskZqRTKzVI> (Lesedato: 5.1.14)

Alver, Bente og Ørjar Øyen (1997): *Forskningsetikk i forskerhverdag: vurderinger og praksis*. Oslo: Tano Aschehoug

Analyse av IKT-styringen i politi- og lensmannsetaten (2013): Brosjyre fra Politidirektoratet.

Bernt, Jan Fridthjof og David R. Doublet (1999) *Juss, samfunn og rettsanvendelse, En introduksjon til rettsvitenskapen*. Oslo: Ad Notam Gyldendal

Boe, Erik (1993): *Innføring i juss. Statsrett og forvaltningsrett*. Bind 2. Oslo: Tano

Chan, Janet (2001): «The Technological Game: How Information Technology is Transforming Police Practice». I: *Criminology and Criminal Justice* Vol. 1(2).

Chan, Janet (2003): «Police and new technologies». I: *Handbook of policing*. Tim Newburn (red.) Cullompton: Willan Publishing

Difi rapport (2013): Innbyggerundersøkelsen 2013. Hva mener brukerne? Difi rapport 2013:7. Oslo: Difi.

Douglas, Mary og Michalis Lianos (2000): «Dangerization and the end of deviance. The institutional environment». I: *Criminology and social theory*. David Garland og Richard Sparks (red.). Oxford: Oxford University Press.

Ericson, Richard V. og Kevin D. Haggerty (1997): *Policing the risk society*. Oxford: Clarendon Press

- Eriksen, Erik Oddvar (2012): «Krigen i hvitt. Om å reparere tillit i organisasjoner» I: *Tillit i Norge*. Helge Skirbekk (red.). Oslo: Res publica
- Et ansvarlig politi*. Oslo: Departementenes servicesenter, informasjonsforvaltning. (NOU 2009: 12)
- Feeley, Malcolm og Jonathan Simon (1998): «Actuarial justice: The emerging new criminal law.» I: *Crime and the risk society*. Pat O'Malley (red.). Dartmouth: Ashgate
- Finstad, Liv (2013): *Politiblikket*. Oslo: Pax Forlag
- Flyghed, Janne (2003): «Den hotfulla säkerheten». I: *Laglöst land*. Janne Flyghed og Magnus Hörnqvist (red). Stockholm: Ordfront
- Flyghed, Janne og Magnus Hörnqvist (2003): «Innledning». I: *Laglöst land*. Janne Flyghed og Magnus Hörnqvist (red). Stockholm: Ordfront
- Foster, Janet (2003): «Police cultures» i: *Handbook of policing*. Tim Newburn (red.) Cullompton: Willan Publishing
- Garland, David (1990): *Punishment and moderen society, a study in social theory*. Oxford: Clarendon press
- Grimen, Harald (2009). *Hva er tillit?* Oslo: Universitetsforlaget
- Grimen, Harald (2012): «Gode institusjoners betydning for tillit». I: *Tillit i Norge*. Helge Skirbekk (red.). Oslo: Res publica
- Gundhus, Helene Oppen (2006): *For sikkerhets skyld. IKT, yrkeskulturer og kunnskapsarbeid i politiet*. Oslo: Unipub
- Hannah-Moffat, Kelly (1999): «Moral Agent or Actuarial Subject: Risk and Canadian Women's imprisonment». I: *Theoretical criminology*, vol 3.
- Hartvigsen, Tore (2013): *Er det behov for nytenkning og utvikling av nye risikoanalysemetoder for å håndtere risiko i det moderne informasjonssamfunn?* Masteroppgave ved UiS
- Hauge, Ragnar (2001): *Kriminalitetens årsaker*. Oslo: universitetsforlaget

Hayward, Keith J. og Jock Young (2004): «Cultural Criminology: Some Notes on the Script». I: *Theoretical Criminology Vol. 8(3)*.

Hudson, Barbara (2003): *Justice in the risk society*. London, Thousand Oaks, New Delhi: Sage Publications

Høigård, Cecilie (2005): *Nytt politi? En kommentert bibliografi over nyere nordisk politiforskning*. K-serien nr. 2/2005.

Innbyggerundersøkelsene. URL: <http://www.difi.no/innbyggerundersokelsen/hva-mener-brukerne>, <http://www.difi.no/innbyggerundersokelsen/hva-mener-brukerne/politi>, <http://www.difi.no/innbyggerundersokelsen-2010> (Lesedato 23.02.14)

Iversen, Torill (2012): *Effektivisering av politiet – nye IKT-løsninger eller økt digital kompetanse?* Masteroppgave ved NTNU

Jansen, Arild og Dag Wiese Schartum (2007): «Elektronisk forvaltning og jus». I: *Elektronisk forvaltning i Norden*. Dag Wiese Schartum (red.) Bergen: Fagbokforlaget

Johannessen, Asbjørn, Per Arne Tufte og Line Kristoffersen (2006): *Introduksjon til samfunnsvitenskapelig metode*, 3. utgave. Oslo: Abstrakt forlag

KS1 konseptvalg (2012): «Kvalitetssikringsfase 1 (KS1 konseptvalg) av fremtidige IKT-systemer til støtte for straffesaksbehandlingen i politi- og påtalemyndigheten.» Rapport til Justisdepartementet og Finansdepartementet. Versjon1.0 Dato: 15. juni 2012. Metier og Møreforskning Molde

Kriminalitetsbekjempelse og personvern. Oslo: Departementenes servicesenter, informasjonsforvaltning. (NOU 2003: 21)

Kvalitetssikringsrapport (2013): «Tilleggsoppdrag kvalitetssikring (ks1) av MERVERDIprogrammet i politiet.» Rapport 6. november 2013. Versjon 1.0. Holte Consulting

Larsson, Paul (2010): «Tillit til politiet. Fra nærhet til forhandlet legitimitet». I: *Tillit til politiet*. Siv R. Runhovde (red.). PHS Forskning 2010: 4. Oslo: Politihøgskolen

Lash, Scott (2000): «Risk Culture». I: *The risk society and beyond. Critical issues for social theory*. Barbara Adam, Ulrich Beck og Joost Van Loon (red.). London, Thousand Oaks, New Delhi: Sage Publications

Lintvedt (2007): «Altinn – en systembeskrivelse». I: *Elektronisk forvaltning i Norden*. Dag Wiese Schartum (red.) Bergen: Fagbokforlaget

Luhman, Niklas (1993): *Risk: a sociological theory*. Berlin – New York: Walter de Gruyter
MERVERDIprogrammet informasjonshefte 2013 – 2014.

Norsk datakunnskap network. URL:

http://www.datamaskin.biz/Systems/windows/216639.html#Uz_FkxQ4XVI (Lesedato 01.04.14)

Northrop, Alana, Kenneth L. Kraemer og John Leslie King (1995): «Police use of computers». I: *Journal of Criminal Justice*, Vol. 23, No. 3.

Politianalysen. Oslo: Departementenes servicesenter, informasjonsforvaltning. (NOU 2013:9)

Politiets nasjonale innbyggerundersøkelse 2010. Rapport i Politidirektoratet 2010. URL:
<http://www.bing.com/search?q=Politidirektoratet+%282009%29.+Politiets+nasjonale+innbyggerunders%C3%B8kelse.+Oslo%3A+TNS+Gallup.&form=IE10TR&src=IE10TR&pc=MAARJS> (Lesedato 23.03.14)

Politi.no URL: https://www.politi.no/om_politiet/organisasjon/ (Lesedato: 04.02.14)

Politihøgskolen.no URL: <http://www.phs.no/studietilbud/bachelor/innhold-i-utdanningen/> (Lesedato 15.03.14)

Politi-loven. Lov om politiet 1995-08-04-53.

Politiregisterloven. Lov om behandling av opplysninger i politiet og påtalemyndigheten 2010-05-28-16.

Punch, Maurice (2003): «Rotten Orchards: “Pestilence”, Police Misconduct and System Failure*». I: *Policing and Society*. Vol. 13, No. 2.

Rachlew, Asbjørn (2010): «Å forske på sine egne. Metodiske og etiske utfordringer knyttet til forskning på egen profesjon». I: *Arbeidsmetoder og metodearbeid i politiet: Forskningskonferansen 2010*. Trond Myklebust og Gunnar Thomassen (red.) Oslo: PHS forskning 2010: 3.

Rapport fra 22. juli-kommisjonen: Oslo: Departementenes servicesenter, informasjonsforvaltning. (NOU 2012: 14)

Reiner, Robert (2003): «Policing and the media». I: *Handbook of policing*. Tim Newburn (red.) Cullompton: Willan Publishing

Reiner, Robert (2013): «Who governs? Democracy, plutocracy, science and prophecy in policing». I: *Criminology and Criminal Justice*, Vol. 13, No. 2.

Riksrevisjonen undersøkelse av ikt-forvaltningen i straffesakskjeden. Dokument 3:12 (2011-2012) Bergen: Fagbokforlaget

Ringdal, Karsten (2001): *Enhet og mangfold*. Bergen: Fagbokforlaget

Robberstad, Anne (1999): *Mellom tvekamp og inkvisisjon. Straffeprosessens grunnstruktur belyst ved fornærmedesstilling*. Oslo: Universitetsforlaget

Rundskriv nr. G-4/2001. URL:

<http://www.regjeringen.no/nb/dep/jd/dok/rundskriv/2001/rundskriv-g-401.html?id=108787>

(Lesedato: 20.02.2014)

Runhovde, Siv R. (2010): «Avslutning». I: *Tillit til politiet*. Siv R. Runhovde (red.). PHS Forskning 2010: 4. Oslo: Politihøgskolen

Schartum, Dag Wiese (1997): «Den kontrollerende forvaltning». I: *Retfærd. Nordisk juridisk tidsskrift* nr.77,20.

Schartum, Dag Wiese (2002): «Fra rettsstat til rettstatsautomat». I: *Digital makt. Informasjons- og kommunikasjonsteknologiens betydning og muligheter*. Tore Slaatta (Red.) Gyldendal Akademisk

Selle, Per og Dag Wollebæk (2012): «Sivilsamfunn og tillit». I: *Tillit i Norge*. Helge Skirbekk (red.). Oslo: Res publica

Shearing, Clifford D. og Philip C. Stenning (1998): «From panopticon to Disney World: the development of discipline». I: *Crime and the risk society*. Pat O'Malley (red.). Ashgate, Dartmouth

Skirbekk Helge (2012): «Tillitens betydning i Norge og Norden» I: *Tillit i Norge*. Helge Skirbekk (red.). Oslo: Res publica

Skirbekk, Helge og Gunnar Skirbekk (2012): «Tillit og mistillit. Norge og Sicilia» I: *Tillit i Norge*. Helge Skirbekk (red.). Oslo: Res publica

Skjult informasjon – åpen kontroll. Oslo: Departementenes servicesenter, informasjonsforvaltning. (NOU 2009: 15).

St.meld. nr. 42 (2004-2005). URL:

<http://www.regjeringen.no/nb/dep/jd/dok/regpubl/stmeld/20042005/stmeld-nr-42-2004-2005-/2.html?id=199244> (Lesedato 07.11.12)

Store norske leksikon. «Rettsikkerhet» URL: <http://snl.no/rettsikkerhet> (Lesedato 23.10.13)

Store norske leksikon. «Kultur» URL: <http://snl.no/kultur> (Lesedato: 24.11.12).

Straffeloven. Lov om straff 2005-05-20-28.

Thagaard, Tove (2003): *Systematikk og innlevelse. En innføring i kvalitativ metode*. Bergen: Fagbokforlaget

Tinholt, Lill Heidi (2013): *Kunnskapsstyrt politiarbeid - i hvilke grad benyttes kunnskapsgrunnlaget i strategisk analyse som styringsverktøy*. Masteroppgave ved Politihøgskolen.

Vaughan, Diane (1999): «The Dark Side of Organizations: Mistake, Misconduct, and Disaster». I: *Annual Review of Sociology*, Vol. 25.

Vaughan, Diane (2004): «Theorizing Disaster: Analogy, historical ethnography, and the Challenger accident». I: *Ethnography* 2004 5: 315.

Virksomhetsstyring (2010): Virksomhetsstyring. Revidert instruks for styring av virksomheter underlagt Politidirektoratet. Instruks av 01.10.2010.

Waddington, P.A.J. (2010): «Police Pursuits: A case study of “Critical Friendship”» I: *Policing*. Volume 4, nr. 2.

Wathne, Christin Thea (2012): «The Norwegian Police Force: a learning organization?» I: *Policing*. Volum 35 nr. 4.

Wollebæk, Dag, Bernard Enjolras, Kari Steen-Johnsen og Guro Ødegård (2012): «Tillit i Norge etter 22. juli» I: *Tillit i Norge*. Helge Skirbekk (red.). Oslo: Res publica

Årsrapport 2010. Spesialenheten for politisaker. Oslo: PJ-trykk

Årsrapport 2013. Spesialenheten for politisaker. Oslo: PJ-trykk

Antall ord i oppgaven⁷: 36532

⁷ Ordtellingen inkluderer ikke sammendrag, abstract, takk, innholdsfortegnelse, fotnoter, litteraturliste og vedlegg

Vedlegg

Vedlegg 1: Intervjuguide straffesakseksperter

Vedlegg 2: Intervjuguide jurist

Vedlegg 3: Intervjuguide bruker

Vedlegg 4: Intervjuguide systemspesialist

Vedlegg 5: Informasjonsskriv

Vedlegg 6: Godkjenning fra NSD

Vedlegg 1: Intervjuguide straffesaksekspert

Innledning

- Kan du kort fortelle om din bakgrunn, hvor lenge har du jobbet i etaten og hvor lenge har du sittet i nåværende stilling?
- På hvilken måte kjenner du til SSP, BOT, og BL/Strasak?

Dagens situasjon og risiko

- I og med at det går for alternativet Nybygg regner jeg med at det er noen utfordringer, problemer eller risiko ved dagens systemer. Kan du fortelle om dette? (Fokus på SSP, BOT og BL/Strasak)
- Er det foretatt risikovurderinger av systemene? Evt hvordan risikovurderinger? Evt hva slags type risiko viste de?
- Kan du si noe om:
 - Identitetsproblematikk (registrering av feil personer eller personer man ikke vet hvem er)
 - Feil i straffeattester pga id, feilregistreringer eller for dårlig kvalitetskontroll ved registrering
 - Ny straffelov som ikke kan tre i kraft
 - Ny politiregisterlov og dens krav
- Vil du si at det er risikabelt å ha utdaterte datasystemer? Hvorfor?
- Hva er de verst tenkelige konsekvensene av utfordringene? Har det noen gang skjedd?
- Hvem rammes av utfordringene? På hvilken måte?
- Vil du si at dagens systemer bidrar til effektivt politiarbeid? (informasjonsdeling/informasjonsuthenting)
- Er informasjonen i dagens systemer fullstendig og korrekte?
- Gir dagens systemer relevant, nøyaktig, pålitelig og etterprøvable statistikk?
- Oppfyller dagens systemer rettslige krav til informasjonssikkerhet og personvern?
- Kan man si at dagens situasjon svekker rettssikkerheten? Da tenker jeg på identitetsproblematikk, straffeattester, lovverk som ikke kan tre i kraft og krav som ikke kan imøtekommes (logging, sporing).

Tiltak utenom merverdiprojektet

- Hvilke tiltak er satt i gang for å bedre situasjonen?
- Finnes det andre tiltak som burde vært satt i gang?
- Hvordan kan gamle utfordringer og eventuelle nye problemer unngås i fremtiden?

Historikk og merverdiprogrammet

- Kan du, i korte trekk, fortelle om historikken rundt arbeidet med nye systemer? Startet det hele når ny straffelov ble vedtatt for første gang, i 2005?

- Hvorfor har det tatt så lang tid å lage nye systemer? (Fra begynnelsen av 2000-tallet.
- Hvilke konsekvenser får det at det tar så lang tid og utvikle nye systemer?
- Nedprioriteres utviklingen av datasystemene? Hvorfor?
- Når kan nye systemer forventes ferdigstilt? Hva menes med ferdig i 2021? I drift, opplæring gjennomført, gamle data konvertert osv?
- Kan du fortelle litt om de nye straffesakssystemene?
- Hvordan er de forskjellig fra de gamle?
- Hva er fordelene?
- Er det ulemper?
- Hvordan vil uttak av statistikk endres i nye systemer?

Årsaksforklaringer

- Hva vil du si er årsaken(e) til at etaten har kommet i en situasjon hvor det er behov for så enorme endringer innen IKT?
- Kan man snakke om en kultur i politiet hvor det ikke er vanlig å innrømme feil eller svakheter?
- Er det ledere, sentrale personer eller andre enkeltpersoner som har stått i veien for utviklingen av nye systemer?
- Har det stort sett vært enighet innad i politiet om hvordan IKT-problemene skal løses?
- Tror du organisasjonsmessige endringer i politiet kunne bidra til en raskere utvikling?
- Er det noen svakheter dere ikke tror det er mulig å rette opp i, som alltid vil være en utfordring?
- Tror du politiet har lært av denne prosessen og at det blir lettere og vedlikeholde og videreutvikle ikt-systemene i fremtiden, slik at det ikke blir en ny krise.

Avslutning

- Tror du IKT-tilstanden fremstilles riktig eller feil i media? Hvordan?
- Synes du at IKT-systemenes tilstand er et politianliggende eller bør alle i samfunnet kjenne til den?
- Hva tror du dagens situasjon gjør med folkets tillit til politiet?
- Er det noe du ønsker å tillegge?

Vedlegg 2: Intervjuguide jurist

Innledning

- Kan du kort fortelle om din bakgrunn og stilling?
- Hvor lenge har du jobbet i etaten?
- Hvor lenge har du sittet i nåværende stilling?
- På hvilken måte kjenner du til SSP, BOT og BL/Strasak?

Dagens situasjon og risiko

- Hvordan vil du si at dagens tilstand er i SSP, BOT og BL/Strasak? Hvilke utfordringer med systemene kjenner du til?
- Hva er de verst tenkelige konsekvensene av utfordringene? Har det noen gang skjedd?
- Hvem rammes av utfordringene? På hvilken måte? Rammes de som er omtalt i systemene? Hvordan? Rammes andre? Hvordan?
- Er det foretatt risikovurderinger av systemene? Hva slags type risiko utgjør dagens systemer? Vil du si at det er risikabelt å ha utdaterte datasystemer? Hvorfor?
- Hva er akseptabel risiko for politiets IKT-systemer? Hvilke typer risiko kan man akseptere og hvilke bør ikke aksepteres?
- Vet du hvor mange personer som har tilgang til de ulike systemene? Er det ulike tilgangsnivåer?
- Hva tror du dagens situasjon gjør med folkets tillit til politiet?
- Kan man si at dagens situasjon svekker rettssikkerheten?
- Vil du si at dagens systemer bidrar til effektivt politiarbeid? (informasjonsdeling/informasjonsuthenting)
- Er informasjonen i dagens systemer fullstendig og korrekte?
- Hvilket system er bakgrunn for uttak av statistikk? Gir dagens systemer relevant, nøyaktig, pålitelig og etterprøvbart statistikk?
- Gir dagens systemer godt grunnlag for rett personidentifisering?

Tiltak

- Hvilke tiltak er satt i gang for å bedre situasjonen?
- Finnes det andre tiltak som burde vært satt i gang?
- Hvordan kan gamle utfordringer og eventuelle nye problemer unngås i fremtiden?

Rettsikkerhet og personvern

- Oppfyller dagens systemer rettslige krav til informasjonssikkerhet og personvern?
 - Hvis nei: Hvilke konsekvenser kan det utløse?
- Er politietaten flinke til å ivareta kravene til personvern i sin bruk av teknologiske løsninger?

- Hender det at systemene skal ivareta ulike behov og disse må gå på bekostning av hverandre? Har du eksempler? Hender det at kontrollaspektet går foran kravet om ivaretagelse av rettssikkerhet eller personvern?
- Har politiet gode rutiner for arkivering, sletting og sporing? Hvordan takler dagens systemer disse kravene?
- Hvordan sikres det at en person ikke registreres flere ganger i et system? Hvilke konsekvenser kan det få hvis en person blir registrert flere ganger? Kan man risikere at straffeattestene blir mangelfulle og direkte feil?
- Hvordan er kravene og rutineene for å dele informasjon om rett identitet/hvilken identitet som skal brukes med andre instanser som for eksempel NAV, folkeregisteret, utlendingsnemda osv?
- Får de som bruker systemene juridisk opplæring? Da tenker jeg innen personvern, strafferett, forvaltningsrett, informasjonssikkerhet osv?

Lovverket

- Hva er årsaken til at ny straffelov ikke har trådt i kraft? Ser du det som et problem? Hvordan?
- Opplever du at det er hull i dagens lovverk med tanke på registrene/systemene?
- Hvis ja: Kan du si noe mer om det? Hva er det loven ikke dekker? Hvorfor dekker ikke loven det området? Hvilke konsekvenser har det?
- Er de ulike ansvarsområdene godt forankret i lovverk og kjent for de ulike aktørene? (Behandlingsansvar, kontroll, videreutvikling, utbedring av tekniske feil)
- Hvorfor har ikke ny politiregisterlov trådd i kraft som planlagt i 2012? Hvilke konsekvenser har det?
- Hvilke endringer medfører loven når den trer i kraft?
- Kan systemene, slik de er i dag, oppfylle kravene i ny politiregisterlov?

Årsaksforklaringer

- Hva vil du si er årsaken(e) til problemene?
- Kan man snakke om en kultur i politiet hvor det ikke er vanlig å innrømme feil eller svakheter?
- Er det ledere, sentrale personer eller andre enkeltpersoner som har stått i veien for utviklingen av nye systemer?
- Har det stort sett vært enighet innad i politiet om hvordan IKT-problemene skal løses?
- Tror du organisasjonsmessige endringer i politiet kunne bidra til en raskere utvikling?
- Er det noen svakheter dere ikke tror det er mulig å rette opp i, som alltid vil være en utfordring?

Tidsaspektet for nye systemer

- Politiet har snakket om at det trengs nye systemer siden begynnelsen av 2000-tallet, hvorfor har det tatt så lang tid å lage nye systemer?
- Er det akseptabelt at det har tatt så lang tid?
- Hvilke konsekvenser får det at det tar så lang tid og utvikle nye systemer?

- Nedprioriteres utviklingen av datasystemene? Hvorfor?
- Når kan nye systemer forventes ferdigstilt?

Avslutning

- Tror du IKT-tilstanden fremstilles riktig eller feil i media? Hvordan?
- Synes du at IKT-systemenes tilstand er et politianliggende eller bør alle i samfunnet kjenne til den?
- Er det noe du ønsker å tillegge?

Vedlegg 3: Intervjuguide bruker

Innledning

- Kan du kort fortelle om din bakgrunn og stilling?
- Hvor lenge har du jobbet i etaten?
- Hvor lenge har du sittet i nåværende stilling?
- På hvilken måte kjenner du til SSP, BOT og BL/Strasak?

Kjennskap til systemene

- Hvor ofte bruker du systemene SSP, BOT og BL/Strasak?
- Hvor mange datasystemer bruker du totalt på en dag?
- I hvilken grad tilbys det opplæring i SSP, BOT og BL/Strasak? Hvordan foregår opplæringen?
- Hvilke(t) system bruker du for å finne ut:
 - Om en person sitter i varetekt/soning?
 - Om en person bruker flere identiteter?
 - En persons straffehistorikk (attest)?
 - Om det foreligger foto/fingeravtrykk/DNA?
 - Informasjon om signalement/utseende?
- Snakker de ulike systemene med hverandre eller med noen andre systemer? Hvis ikke: Hvilke konsekvenser har det? Kan det som registreres i systemene få betydning i andre systemer?
- Hvor nøye er man ved registrering og kvalitetskontroll i de ulike systemene?
- Hvor mange systemer må du gjøre endringer i hvis du skal endre registrert identitet på en person? Hvis flere enn 1: Kan det være problematisk hvis du glemmer å oppdatere noen steder? Hvordan?
- Hvordan sikres det at en person ikke registreres flere ganger i et system? Hvilke konsekvenser kan det få hvis en person blir registrert flere ganger?
- Hvordan er rutineene for å dele informasjon om rett identitet/hvilken identitet som skal brukes med andre som NAV, folkeregisteret, utlendingsnemda osv?
- Registreres en person en eller flere ganger i BOT og BL/Strasak? Oppdateres systemene hvis en person endrer identitet eller det avdekkes falsk identitet?

Dagens situasjon og risiko

- Hvordan vil du si at dagens tilstand er i SSP, BOT og BL/Strasak? Hvilke utfordringer med systemene kjenner du til?
- Hva er de verst tenkelige konsekvensene av utfordringene? Har det noen gang skjedd?
- Hvem rammes av utfordringene? På hvilken måte? Rammes de som er omtalt i systemene? Hvordan? Rammes andre? Hvordan?
- Er det foretatt risikovurderinger av systemene? Hva slags type risiko utgjør dagens systemer? Vil du si at det er risikabelt å ha utdaterte datasystemer? Hvorfor?
- Vet du hvor mange personer som har tilgang til de ulike systemene? Er det ulike tilgangsnivåer?
- Hva tror du dagens situasjon gjør med folkets tillit til politiet?
- Kan man si at dagens situasjon svekker rettssikkerheten?

- Vil du si at dagens systemer bidrar til effektivt politiarbeid? (informasjonsdeling/informasjonsuthenting)
- Er informasjonen i dagens systemer fullstendig og korrekte?
- Gir dagens systemer relevant, nøyaktig, pålitelig og etterprøvbar statistikk?
- Oppfyller dagens systemer rettslige krav til informasjonssikkerhet og personvern?
- Gir dagens systemer godt grunnlag for rett personidentifisering?
- Tror du utseende på dagens systemer kan bidra til å svekke brukernes tillit til det? Skjønner man at noe som ser utdatert ut kan inneholde oppdatert informasjon?

Tiltak

- Hvilke tiltak er satt i gang for å bedre situasjonen?
- Finnes det andre tiltak som burde vært satt i gang?
- Hvordan kan gamle utfordringer og eventuelle nye problemer unngås i fremtiden?

Tidsaspektet

- Politiet har snakket om at det trengs nye systemer siden begynnelsen av 2000-tallet, hvorfor har det tatt så lang tid å lage nye systemer?
- Er det akseptabelt at det har tatt så lang tid?
- Hvilke konsekvenser får det at det tar så lang tid og utvikle nye systemer?
- Nedprioriteres utviklingen av datasystemene? Hvorfor?
- Når kan nye systemer forventes ferdigstilt? I drift, opplæring gjennomført, gamle data konvertert osv?

Årsaksforklaringer

- Hva er årsaken(e) til problemene?
- Kan man snakke om en kultur i politiet hvor det ikke er vanlig å innrømme feil eller svakheter?
- Er det ledere, sentrale personer eller andre enkeltpersoner som har stått i veien for utviklingen av nye systemer?
- Tror du organisasjonsmessige endringer i politiet kunne bidra til en raskere utvikling?
- Er det noen svakheter dere ikke tror det er mulig å rette opp i, som alltid vil være en utfordring?

Avslutning

- Tror du IKT-tilstanden fremstilles riktig eller feil i media? Hvordan?
- Synes du at IKT-systemenes tilstand er et politianliggende eller bør alle i samfunnet kjenne til den?
- Er det noe du ønsker å tillegge?

Vedlegg 4: Intervjuguide systemspesialist

Innledning

- Kan du kort fortelle om din bakgrunn, hvor lenge har du jobbet i etaten og sittet i nåværende stilling?
- På hvilken måte kjenner du til SSP, BOT, BL og Strasak? Har du jobbet med saksbehandling i systemene eller vært med å utvikle eller vedlikeholde dem?

Dagens situasjon og risiko

- I og med at det går for alternativet nybygg regner jeg med at det er noen utfordringer, problemer eller risiko ved dagens systemer. Kan du fortelle om dette? (Fokus på SSP, BOT og BL/Strasak)
- Hva er de verst tenkelige konsekvensene av utfordringene? Har det noen gang skjedd?
- Hvem rammes av utfordringene? På hvilken måte? Rammes de som er omtalt i systemene? Hvordan? Rammes andre? Hvordan?
- Er det foretatt risikovurderinger av systemene? Hva slags type risiko utgjør dagens systemer?
- Vil du si at det er risikabelt å ha utdaterte datasystemer? Hvorfor?
- Hva er akseptabel risiko for politiets IKT-systemer? Hvilke typer risiko kan man akseptere og hvilke bør ikke aksepteres?
- Kan du si noe om:
 - Identitetsproblematikk (registrering av feil personer eller personer man ikke vet hvem er)
 - Feil i straffeattester pga id, feilregistreringer eller for dårlig kvalitetskontroll ved registrering
 - Ny straffelov som ikke kan tre i kraft
 - Ny politiregisterlov og dens krav
- Hva tror du dagens situasjon gjør med folkets tillit til politiet?
- Kan man si at dagens situasjon svekker rettssikkerheten?
- Vil du si at dagens systemer bidrar til effektivt politiarbeid? (informasjonsdeling/informasjonsuthenting)
- Er informasjonen i dagens systemer fullstendig og korrekte?
- Hvilke systemer er bakgrunn for uttak av statistikk? Gir dagens systemer relevant, nøyaktig, pålitelig og etterprøvbart statistikk?
- Tror du utseende på dagens systemer kan bidra til å svekke brukernes tillit til det? Skjønner man at noe som ser utdatert ut kan inneholde oppdatert informasjon?

Tiltak utenom merverdiprogrammet

- Hvilke tiltak er satt i gang for å bedre situasjonen?
- Finnes det andre tiltak som burde vært satt i gang?
- Hvordan kan gamle utfordringer og eventuelle nye problemer unngås i fremtiden?

Årsaksforklaringer

- Hva er årsaken(e) til problemene?
- Kan man snakke om en kultur i politiet hvor det ikke er vanlig å innrømme feil eller svakheter?
- Er det ledere, sentrale personer eller andre enkeltpersoner som har stått i veien for utviklingen av nye systemer?
- Har det stort sett vært enighet innad i politiet om hvordan IKT-problemene skal løses?
- Tror du organisasjonsmessige endringer i politiet kunne bidra til en raskere utvikling?
- Er det noen svakheter dere ikke tror det er mulig å rette opp i, som alltid vil være en utfordring?

Utviklere ved PDMT

- Er det fast ansatte eller innleide konsulenter som utvikler de nye systemene?
- Etter at et ikt-system er ferdig utarbeidet, hvordan er rutinene for oppfølging/vedlikehold og videreutvikling?
- Hvor mange hos PDMT kan SSP, BL/Strasak og BOT godt?
- Er det noen som kan systemene godt hvis det var innleide konsulenter som utviklet dem?

Tidsaspektet

- Politiet har snakket om at det trengs nye systemer siden begynnelsen av 2000-tallet, hvorfor har det tatt så lang tid å lage nye systemer? Er det akseptabelt at det har tatt så lang tid?
- Hvilke konsekvenser får det at det tar så lang tid og utvikle nye systemer?
- Nedprioriteres utviklingen av datasystemene? Hvorfor?
- Når kan nye systemer forventes ferdigstilt?

Avslutning

- Tror du IKT-tilstanden fremstilles riktig eller feil i media? Hvordan?
- Synes du at IKT-systemenes tilstand er et politianliggende eller bør alle i samfunnet kjenne til den?
- Er det noe du ønsker å tillegge?

Vedlegg 5: Informasjonsskriv

Informasjonsskriv

Jeg er student ved Universitetet i Oslo og skal skrive masteroppgave om IKT-situasjonen i politiet. Ved siden av studiene jobber jeg som førstekonsulent på Kripos, men det presiseres at masteroppgaven er et studentprosjekt. Kripos er informert om prosjektet.

Temaet for masteroppgaven er konsekvenser av politiets IKT-situasjon med fokus på SSP, BOT og BL/Strasak. Målet med oppgaven er å bidra til økt forståelse av dagens IKT-situasjon og peke på mulige utfordringer ved systemene og lovverket. Jeg ønsker å belyse dette for å unngå at eventuelle problemer som foreligger i dag gjentas i nye systemer.

Målet mitt er å intervju en fra PDMT, en fra Kripos, en fra MERVERDIprogrammet og en som bruker systemene daglig. Jeg ønsker deg som informant fordi jeg tror du har kunnskap om lovverket, systemene eller bruken av systemene som kan gi meg svar på mine forskningsspørsmål.

Ditt navn og stillingstittel vil være anonym, men det vil fremkomme hvor du jobber. Intervjuet vil bli tatt opp med lydopptaker. Opplysningene fra opptakene anonymiseres og slettes når oppgaven er ferdig, innen 01.07.14.

Ved å skrive under på dette dokumentet samtykker du til at du har fått informasjon om forskningsprosjektet og mine mål. Samtykkeerklæringen kan gis til meg ved intervjuet. Hvis det er ønskelig har du anledning til å trekke deg som informant når som helst, frem til prosjektet ferdigstilles. Ønsker du mer informasjon før du skriver under kan du ringe meg på tlf. 951 20 274, eller sende e-post til f.f.wold@student.jus.uio.no. Du kan også kontakte min veileder Liv Finstad ved institutt for kriminologi og retts sosiologi på tlf. 22 85 01 18. Mer informasjon kan gis både muntlig og skriftlig.

Prosjektet er meldt til Personvernombudet for forskning, Norsk samfunnsvitenskapelig datatjeneste (NSD).

Mvh

Frøydis Wold
Midtveien 25
1458 Fjellstrand

Samtykkeerklæring

Jeg har mottatt skriftlig informasjon og er villig til å delta i studien.

Dato..... Signatur.....

Vedlegg 6: Godkjenning fra Norsk samfunnsvitenskapelig datatjeneste

Liv Finstad
Institutt for kriminologi og rettssosiologi
Universitetet i Oslo
Postboks 6706 St. Olavs plass
0130 OSLO

Vår dato: 07.01.2013

Vår ref:32564 / 3 / LT

Deres dato:

Deres ref:

TILBAKEMELDING PÅ MELDING OM BEHANDLING AV PERSONOPPLYSNINGER

Vi viser til melding om behandling av personopplysninger, mottatt 02.01.2013. Meldingen gjelder prosjektet:

32564	<i>Shit in - shit out. Mulige rettsikkerhetsmessige konsekvenser av politiets IKT-situasjon</i>
Behandlingsansvarlig	Universitetet i Oslo, ved institusjonens øverste leder
Daglig ansvarlig	Liv Finstad
Student	Frøydis Wold

Personvernombudet har vurdert prosjektet og finner at behandlingen av personopplysninger er meldepliktig i henhold til personopplysningsloven § 31. Behandlingen tilfredsstiller kravene i personopplysningsloven.

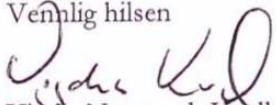
Personvernombudets vurdering forutsetter at prosjektet gjennomføres i tråd med opplysningene gitt i meldeskjemaet, korrespondanse med ombudet, eventuelle kommentarer samt personopplysningsloven og helseregisterloven med forskrifter. Behandlingen av personopplysninger kan settes i gang.

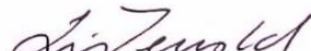
Det gjøres oppmerksom på at det skal gis ny melding dersom behandlingen endres i forhold til de opplysninger som ligger til grunn for personvernombudets vurdering. Endringsmeldinger gis via et eget skjema <http://www.nsd.uib.no/personvern/meldeplikt/skjema.html>. Det skal også gis melding etter tre år dersom prosjektet fortsatt pågår. Meldinger skal skje skriftlig til ombudet.

Personvernombudet har lagt ut opplysninger om prosjektet i en offentlig database, <http://pvo.nsd.no/prosjekt>.

Personvernombudet vil ved prosjektets avslutning, 01.07.2014, rette en henvendelse angående status for behandlingen av personopplysninger.

Vennlig hilsen


Vigdis Namtvedt Kvalheim


Lis Tenold

Lis Tenold tlf: 55 58 33 77

Vedlegg: Prosjektvurdering

Kopi: Frøydis Wold, Vestoppfaret 1b, 1450 NESODDTANGEN



Opplysningene samles inn gjennom intervju. Intervjuene tas opp på lydbånd og behandles elektronisk.

Det gis skriftlig informasjon og innhentes skriftlig samtykke. Personvernombudet finner skrivet godt utformet.

Innsamlede opplysninger registreres på privat pc. Personvernombudet forutsetter at bruk av minnepenn og privat pc er i tråd med Universitetet i Oslo sine interne retningslinjer for informasjonssikkerhet.

Innsamlede opplysninger anonymiseres og lydbåndopptak makuleres ved prosjektslutt, senest 01.07.2014. Med anonymisering innebærer at navnelister slettes/makuleres, og ev. kategorisere eller slette indirekte personidentifiserbare opplysninger. Ved publisering vil ingen enkeltpersoner kunne gjenkjennes