Politiets forebygging av terrorisme via "datagraving"– vil målet hellige midlene?

En teoretisk oppgave

Bacheloroppgave (OPPG300)

Politihøgskolen

2014

Kandidat nr.: 459

Antall ord: 6.600

Innholdsfortegnelse

1 Innledning

Terrorisme fremstår som en av vår tids alvorligste utfordringer, og handlingsviljen for å bekjempe terrorisme har sannsynligvis aldri vært sterkere. Det er et uttalt mål at politiet skal jobbe kunnskapsbasert og forebyggende, herunder i politianalysen som ble lagt fram 19.juni 2013(NOU 2013:9). Politiloven §2 nr.1 sier at det er samfunnets behov for trygghet som står i hovedfokus for politiets virksomhet(Myhrer,2011,s.16). Nr.2&3 sier at dette blant annet skal gjøres ved å forebygge, avdekke og stanse kriminell virksomhet.

Terrorisme er på ingen måte et nøytralt begrep, men et begrep med diffuse grenser. Det er en flytende overgang mellom terrorisme og en rekke andre handlinger. Det er avhengig av "øyet som ser", og i tråd med Aadlands beskrivelse av subjektiv sannhet(2011,s.75). En felles definisjonen av terrorisme er derfor en grunnleggende forutsetning for å fastslå om en handling er terrorisme eller ei. Jeg har i oppgaven benyttet meg av Nordenhaug&Engene´s (2008,s.15) definisjon, som sier at terrorisme er

"*Voldsbruk som med overlegg rammer sivile for å skape en effekt på andre*".

Terrorhandlinger har ført til at myndighetene går nye veier for å sikre trygghet. Samtidig setter den teknologiske utviklingen, med bruk av internett og publikums-genererte data, personvernet under sterkt press. Mange av de store tiltakene gjennomføres med argument å skulle forebygge terrorisme. Ved å "patruljere og grave" i publikums data(derav utrykket "**datagraving**") kan man oppdage svært mye kriminalitet FØR og mens det skjer, noe som påpekes i rapporten fra 22.juli-kommisjonen(NOU 2012:14). Denne formen for datagraving er en form for elektronisk gjennomgang av befolkningens data, der det i utgangspunktet ikke foreligger noen "skjellig grunn" til å mistenke noe kriminelt. Dette kaller Lie situasjonell forebygging, som innebærer å begrense muligheten for å begå kriminalitet ved å gjøre noe med situasjonen(2011,s.252).

I praksisåret hadde jeg mange diskusjoner med kollegaer rundt myndighetenes overvåking av samfunnet og dets borgere. Stort sett alle var tilhengere av økt overvåking. Vi ser ofte på overvåking som positivt, for så lenge man er lovlydig har man heller ikke noe å frykte. Da ser man bort fra hvor sensitiv personinformasjon er, og hvor mye makt den kan gi innehaveren av

informasjonen. Den siste tidens overvåkingsavsløringer, og fokus på Datalagrinsdirektiv, har gjort meg mer skeptisk til overvåking. Det har fått meg til å åpne øyne, og se på overvåking på en annen måte.

1.1 Problemstilling

> *Hvilke dilemmaer kan oppstå ved politiets bruk av datagraving i publikums data, der formålet er å forebygge terrorisme?*

Jeg vil i oppgaven ha en gjennomgående drøfting av politiets datagraving for å forebygge terrorisme. Jeg vil vise til hva norsk lovverk sier om dette, og se på den norske terrortrusselen. Jeg vil videre drøfte hvilke negative konsekvenser datagraving kan ha for personvern. Jeg vil på den måten vurdere både positive og negative sider ved datagraving som virkemiddel for å forebygge terrorisme.

1.2 Avgrensning

Oppgaven er begrenset til kriminalitet i form av terrorisme.

Forebyggingsbegrepet er et vidt definert begrep. Hovedfokus vil være på situasjonell forebygging, da det først og fremst er dette forebyggingsprinsippet datagraving hører inn under. Personorientert forebygging vil omhandles i mindre grad, mens gjenopprettende rett ikke blir omhandlet. Lokalorientert forebygging er viktig, og kunne vært et eget tema. Det blir likevel ikke omhandlet grunnet plassbegrensning.

1.3 Oppbygning av oppgaven

Oppgaven er delt i tre hovedkapitler (kapt.3-5):

Innledningsvis vil jeg i kapt.3 beskrive hvordan samfunnet digitaliseres, og hvordan tilgang på data kan gi kunnskap og makt. Her vil jeg beskrive proaktiv politiarbeid, og mulighet for bruk av Internett og datagraving som kunnskapsbasert politiarbeid(Lie,2011,s.324).

Deretter vil jeg beskrive datagraving som situasjonell forebyggingstiltak, og vise eksempler på positive- og negative forskyvningseffekter. Her vil jeg også vise til hvordan

personorientert forebygging kan benyttes parallelt med den situasjonelle for å få større utbytte.

Jeg vil videre knytte datagraving opp mot et av de mest omfattende terrortiltakene som er planlagt i Norge i nærmeste framtid: innføringen av EUs Datalagringsdirektiv. Dette vil jeg se opp mot personvernet, som står en grunnleggende rettighet i det norske demokratiet. Dette gjøres for å skape en motpol mot bruken av datagraving som "tvangstiltak" mot vanlige borgere. Her vil jeg også se på lovverket for politiets bruk av datagraving, knyttet opp mot forebygging av terrorisme.

Fordi hovedformålet med datagraving er å forebygge terrorisme, vil jeg i kapittel 4 redegjøre for nåtidens terrorbølge(Nordenhaug&Engene,2008) og beskrive trusselbildet mot Norge(PST,2014). På den måten vil man lettere kunne se om terrortiltak samsvarer med terrortrussel.

Til slutt vil jeg i kapt.5 stille datagraving og personvern opp mot hverandre, og drøfte hvilke negative konsekvenser datagraving kan ha for personvern.

2 Metode

2.1 Teoretisk oppgave og selvvalgt pensum

Jeg har valgt å skrive en teoretisk oppgave. Dette er en type oppgave der man besvarer og diskuterer faglige spørsmål med utgangspunkt i eksisterende litteratur og skrevne kilder (Dalland,2012).

I denne teoretiske oppgaven ønsker jeg å drøfte bruken av datagraving i publikums data for å forebygge terrorisme. Jeg vil referere til Nordenhaug&Engene(2008) og Bjørgo(2011), som har forsket på bekjempelse av terrorisme i Norge. Dette vil jeg se opp mot eksisterende lovverk og negative konsekvenser for personvern.

Datagraving er et relativt nytt begrep det er skrevet lite om. Her har jeg sett på Hammerlins(2009) synspunkter rundt et kontrollsamfunn som er under utvikling. Jeg vil bruke kreative innfallsvinkler og fortolkninger, som bygger på vitenskapelige undersøkelse og faglig innsikt. Jeg vil se på dette i et politifaglig-, juridisk- og kriminologisk perspektiv.

2.2 Forforståelse og kildekritikk

Alt vi opplever og mottar av inntrykk blir fortolket av oss selv ut fra våre fordommer og forforståelser, slik at det som av noen kalles objektiv kunnskap i siste instans ender opp som våre personlige fortolkninger(Aadland,2011,s.74). Via omgang med andre mennesker blir vi på den måten sosialisert til det som kalles forforståelse.

Forforståelse er nødvendig i all forskning for å kunne innhente relevante data. Forskerens forforståelse vil kunne påvirke hva forskeren observerer, og hvordan disse observasjonene vektlegges og tolkes. Det er viktig med en bevisstgjøring av forforståelsen, da den er med på å fargelegge våre oppfatninger. Den kan setter grenser for vår kreativitet, mangfoldighet og forestillingsevne(Aadland,2011).

Mye av min forforståelse har jeg fra tidligere yrke og utdanning. Jeg har en cand.mag-grad fra Ifi[1], og har jobbet i over 10 år som systemutvikler i offentlige- og private prosjekt. Personvern er noe jeg har hatt fokus på. Min interesse for fagfeltet har ytterligere blitt forsterket via medias søkelys på de ulike overvåkingsskandalene i verden. Et spesielt inntrykk har avsløring om at den amerikanske etterretningsorganisasjonen NSA har utført storstilt overvåking av privatpersoner i store deler av verden, deriblant Norge. Via datagraving har etterretningstjenesten fått direkte tilgang til nordmenns personopplysninger. Totalomfanget er fremdeles ukjent, men avisen skriver at NSA har fått tilgang på informasjon som gjør at de har kjennskap til alt en person gjør på nettet. Dette gjelder både bruk av lyd, video, fotografier, epost og nettlogger(Vestrum,2013).

Etter avsløringen har det vært enorm mediefokus på politiets overvåking, med de konsekvenser dette har for publikum. Dette mediebildet har vært med på å påvirke mine oppfatninger. Datagraving er ”ny” teknologi, med mange ubesvarte spørsmål, og uklart

[1] **Ifi**: **I**nstitutt **f**or **i**nformatikk ved Universitetet i Oslo(UiO).

regelverk. Jeg har vært i kontakt med sentrale aktører i Datatilsynet, forfatter av kildelitteratur, aktører innenfor overvåkning i Norge, og forskere innenfor informatikk og internett. Valg av problemstilling, tematisering, og ikke minst Hammerlin(2009), Bjørgo(2011) og Nordenhaug&Engene(2008) som selvvalgt pensumlitteratur, er påvirket av min forforståelse. Bevisstgjøring om at disse valgene ikke er verdifrie og nøytrale er viktig.

For å belyse den faktiske faren for å bli rammet av terrorisme har jeg undersøkt terrortallene i verden(START,2012). Bruk av statistikk vil ikke bli påvirket av forforståelse, da tallene er basert på et objektive tallmateriale. Det kan likevel eksistere mørketall som statistikken ikke fanger opp. Dette kan være med på å gi et feil bilde av virkeligheten. Statistikkgrunnlagets definisjon av terrorisme vil også kunne påvirke resultatet. I uttrekket av data i mitt studie har jeg basert meg på definisjonen av terrorisme presentert innledningsvis.

3 Kunnskap er makt

"Kunnskap er makt, særlig kunnskap om andre mennesker".

Sitatet stammer fra J. Edar Hoover, mannen som fungerte som direktør for FBI i 48 år(sitert i Hammerlin,2009,s.44). I dagens samfunn, hvor mer og mer informasjon blir digitalisert, handler makt om tilgang og kontroll på data.

Etter 11.september 2001 har Norge innført rettslige tiltak som tidligere ble vurdert som problematiske. De nye strafferettslige tiltakene av 2008 er rettet mot "oppfordring og forberedelse" til terrorisme(St.meld.nr.61). Samtidig skal det innføres nye tiltak, som eksempelvis Datalagringsdirektivet, som kan brukes til å forebygge terrorisme. Denne formen for forebyggende politivirksomhet kalles "proaktiv politivirksomhet".

3.1 Proaktiv politiarbeid

I boka "Norge i kamp mot terrorisme" har Nordenhaug&Engene(2008) analysert hovedlinjene i norsk terrorbekjempelse fra 1993 og fram til 2008. Terrorhandlingen i USA 11.september 2001 beskrives som et veiskille for norsk antiterrorpolitikk, der politikken dreier seg fra passivitet til proaktivitet. Formålet er å oppnå en forebyggende effekt ved å gjøre terroristenes

virksomhet vanskeligere, komme terroristene i forkjøpet og avdekke eller avverge terrorhandlinger før de skjer(2008,s.40).

På sitt beste kan slik forutseende politiarbeid være en metode som presist kan fortelle noe om kriminalitetsbildet. Dermed kan politiet sette inn ressursene der det trengs. Dette vil kunne gi et mer målrettet politi, som i større grad kan være ”*i forkant*” av situasjoner. Dette vil være både tids- og kostnadsreduserende, noe som gjør at Norge som samfunn kan få mer politi for pengene.

3.2 Kunnskapsbasert politiarbeid

Internett er et verdensomspennende datanettverk med utallige muligheter. Her eksisterer det ingen landegrenser, fysiske murer eller passkontroll. Det brukes av alle samfunnsinstanser, i alle sammenhenger, over hele verden. Vi bruker nettet som privatperson, familie, arbeidstager og samfunn. Nettet er ofte det første vi kobler oss opp mot når vi står opp om morgenen, og det siste vi logger oss av før vi legger oss for kvelden. Internett er blitt det viktigste hjelpemidlet for informasjonsspredning, kommunikasjon, handel og forvaltning. Det er knapt noe bruksområde som ikke kan utføres via nettet i dag.

Stadig større deler av det vi foretar oss lagres og digitaliseres(Frønes,2011). I løpet av en normal dag legger nordmenn igjen store mengder elektroniske spor. Når man ringer og sender SMS, når man surfer på Internett, når man sender epost, når man betaler med bankkort og når man passerer bomstasjoner. Slike lagrede spor kalles ”**metadata”**, og er automatisk genererte opplysninger som sier noe om konteksten av kommunikasjon som blir snappet opp(Bleikelia,Færaas&Johansen,2013). Offentlige organer registrerer omhyggelig både stort og smått om vår ferd fra fødsel til død, banken kjenner vår økonomi og våre handlevaner, og et utall næringsdrivende har mye informasjon i sine kunderegistre(Knoph&Lilleholt,2004, s.104). Datateknikken åpner for nærmest ubegrensede muligheter, noe politiet kan bruke i etterretningsøyemed til å kartlegge bevegelsesmønstre, sosiale nettverk, venner og interesser. Dette er det Lie kaller for kunnskapsbasert kriminalitetsforebygging, og er en vitenskapeliggjøring av politiets forebyggende arbeid som er knyttet til informasjonsinnhenting(2011,s.325).

Datatilsynet refererer **Big Data** til et enormt datasett med slike metadata(Datatilsynet,2012a), og representerer et paradigme-skifte ved etterretningsarbeid. Metadata om publikum kan samles inn fra mange ulike kilder. Dette kan være både fra åpne kilder på nettet, eller fra mer lukkede kilder som produserer metadata på bakgrunn av publikums handlinger. Eksempel på dette er banktransaksjoner. Dataene kan deretter analyseres i helt nye sammenhenger. Dataprogrammer kan "spise" gjennom enorme datamengder på kort tid, og omgjøre dette til forutsigbar analyse om hvem og hvor terrorisme kommer til å skje. På den måten kan man ha en fremtidig beredskapstankegang, der man ved å være "i forkant" kan stanse en planlagt terrorhendelse.

3.3 Situasjonell forebygging

Utviklingen av IKT[2]-basert kommunikasjon kommer til å fortsette å revolusjonere måten vi lever på i overskuelig framtid. Med politiøyne åpner dette for nye muligheter, som setter forebyggende politiarbeid i et helt nytt lys.

Det er først og fremst situasjonelle forebygging datagraving hører inn under, ved å begrense muligheten for å begå kriminalitet. Utgangspunktet for dette perspektivet er at uønskede handlinger utløses i konkrete situasjoner, og at man ved å gripe inn i selve situasjonen kan forhindre at handlingene blir utført(Lie,2011,s.252).

De fleste terroristhandlinger krever en viss form for forberedelse. Her kan nevnes planlegging, innkjøp, koordinering og kommunikasjon mellom eventuelle aktører. Dette lar seg vanskelig gjøre i dag uten å legge fra seg digitale spor(Frønes,2011). Via datagraving vil slike digitale spor kunne oppdage terrorisme allerede på planleggingsstadiet, og dermed forhindre gjennomføringsevnen. På den måten gjør man det vanskelig for terroristen ved å øke oppdagelsesrisikoen, anstrengelsene og mulighetene for å gjennomføre terrorhandlinger(Lie,2011). Mens de fleste forebyggingstiltak forsøker å påvirke aktører direkte, forsøker situasjonelle forebyggingstiltak å påvirke aktørene indirekte ved å endre situasjonene handlingene foregår i(Bjørgo,2011,s.47). Strategien søker å gripe inn mot de forholdene som muliggjør en kriminell handling, slik at man avskrekkes og avstår fra å begå den kriminelle handlingen(Bjørgo,2011,s.19). Denne formen for situasjonell

[2] **IKT**: **I**nformasjon- og **k**ommunikasjons**t**eknologi.

forebyggingstiltak er rettet inn mot å redusere terroristhandlinger, og ikke påvirke terroristens generelle motivasjon(Bjørgo,2011,s.49).

En stor forskjell mellom datagraving som situasjonell forebyggingstiltak og andre forebyggingsprinsipper, er at publikum i ingen grad er involvert i virksomheten. Datagraving krever ingen samarbeid eller "teamtenkning", og involverer i seg selv ingen tverrfaglige etater. Datagravingen kan redusere mennesket til summen av de digitale sporene vi legger igjen. Mennesket blir i så måte tingliggjort i det Skjervheim beskriver som "det industrielle mistaket"(sitert i Christoffersen,2011,s.53). Vi blir våre data!

3.4 Omfordelingseffekt

Som situasjonell forebyggingsstrategi er datagraving ikke en metode for å redusere drivkreftene og motivasjonen for å ta i bruk terrorisme som virkemiddel. Dette må politiet være bevist på, slik at den kriminelle ikke finner andre arenaer hvor datagravingen ikke når dem, såkalt negativ omfordelingseffekt(Lie,2011,s.264). Når terrorisme blir vanskeliggjort på et område vil problemene kunne forflytte seg til andre områder. Lie nevner fem måter forflytning vil kunne skje(2011,s.265): Geografisk, temporært, mål, taktisk og kriminalitetstype. Terrorisme vil eksempelvis kunne forflyttes geografisk til områder med mindre digital kontroll, eller bli mer spontane og mindre planlagt slik at digitale spor ikke legges igjen.

På 1970- og 1980-tallet var flykapring en vanlig terroristmetode(Nordenhaug&Engene,2008, s.25). Etter omfattende situasjonelle forebyggingstiltak, deriblant på flyplasser, er flykapring i dag nesten fraværende. Likevel eksisterer terrorisme i dag, men i andre "former og utgaver". Da flykapring ble vanskeliggjort fant terroristen andre arenaer å utføre sine handlinger på. En lignende omfordelingseffekt vil man kunne oppleve ved bruk av datagraving. Dette må man være bevist på, slik at terrorisme ikke dukker opp et annet sted eller i en annen form som kanskje er verre enn den vi opprinnelig hadde. En viktig oppgave må derfor være å benytte andre forebyggingsstrategier parallelt med de situasjonelle. Eksempler på dette kan være å

forsøke å fjerne grunnleggende årsaker og frustrasjoner som bunner ut i terroristhandlinger, samt å stanse radikaliseringsprosesser[3] på et tidlig stadium.

På den andre siden kan vi få en positiv omfordelingseffekt ved at terroristene tror at datagraving som situasjonelt tiltak er mer effektivt enn det faktisk er(Lie,2011,s.266). Lie viser til flere eksempler hvor situasjonelle tiltak har fått langt større positiv effekt utover områdene de er satt inn. Lie forklarer dette med avskrekking og redusert attraktivitet, der gjerningsmannen overdriver tiltakenes omfang slik at troen på en vellykket gjennomføring blir redusert mer enn nødvendig(2011,s.266).

3.5 Personorientert forebygging

Ved å identifisere mulige terroristaktører kan man stoppe terroristhandlinger FØR planene iverksettes. Deretter kan man forsøke å påvirke de bakenforliggende årsaker til at et individ ønsker å utføre terror. Dette er det Lie kaller for personorientert kriminalitetsforebygging (2011,s.60). Den tar sikte på å identifisere risikopersoner, og deretter sette inn hensiktsmessige tiltak for å redusere drivkreftene og motivasjonen for å ta i bruk terrorisme som virkemiddel. Personorientert forebygging blir dermed en dreining fra generell forebygging til en ”spissing” mot de som er i faresonen. Hensikten med datagraving er å lete etter mønster og sammenhenger det tidligere var umulig å få øye på, og deretter lage profiler på enkeltgrupper og -personer. Ut fra den samlede informasjonen kan politiet opprette tiltak mot individer og grupper. Her kan nevnes at Politiets Sikkerhetstjeneste(PST) har bekymringssamtaler med ungdom i muslimske miljøer på vei inn i radikalismen (Hopperstad&Johnsen,2013).

Bekymringssamtalen er en personorientert dialog- og karleggingssamtale, som retter seg både mot risikoindividet og dennes familie(Politidirektoratet,2011). Dette er et forebyggende verktøy, og ikke en del av straffesaksbehandlingen eller alternativ til straff. Målet er å sikre god oppfølging av individets livssituasjon, stanse negativ atferdsmønster og komme fram til gode løsninger. I sammenheng med terrorisme handler det om å få en oversikt over risikofaktorer, finne årsaker til radikalisering og tydeliggjøre konsekvenser. Mye av det

[3] **Radikalisering**: ”Prosessen der en person i økende grad aksepterer bruk av vold for å nå sine politiske mål”(Meld.St. 21).

forebyggende aspektet ligger dessuten i å måtte møte hos politiet. På den måten utfører man personorientert forebygging ved å informere om at det er en farlig vei personen beveger seg inn på, samtidig som man gjør denne oppmerksom på at politiet følger med. Slike bekymringssamtaler må også sees i sammenheng med kunnskapsbasert politiarbeid, der samtalens etterretningsverdi vil kunne gi mulighet til å iverksette forebyggende tiltak sett i et helhetsperspektiv(Politidirektoratet,2011). Dette er altså et eksempel på hvordan datagraving som situasjonell forebyggingstiltak kan brukes til å identifisere terroraktører, og hvordan personorientert forebygging via bekymringssamtalen kan forebygge videre. Det er for øvrig viktig å være bevist på at bekymringssamtalen ikke er et etterretningsverktøy, men et forebyggende verktøy.

Her må man trå forsiktig slik at personen ikke blir stemplet[4] av nærmiljøet, noe som igjen kan føre til en stigmatiseringsprosess[5]. Dette kan resultere i at personens selvbilde endres, noe som kan danne grobunn for selvoppfyllende profetier. Christoffersen stiller spørsmål om det mellom linjene i politikken er krav om at de som er annerledes skal bli som oss(2011,s.38)? Han sier videre at behandling av avvikere ofte har vært brutale overgrep, med sikte på å tvangs-innordne dem inn i en "moderne og sivilisert" livsform. Hauge sier at når en person defineres som avviker, vil dette virke inn på hvordan vi oppfatter og opptrer ovenfor ham eller henne(2007,s.377).

Radikalisering vil også kunne føre til marginalisering[6]. Mennesker kan eksempelvis havne i gråsonen mellom integrasjon og ekskludering(Fauske&Øya,2010,s.231), for på den måten stå uten et klart fotfeste i noen leir. Dermed kan man bli ekskludert fra viktige sosiale arenaer og virksomheter, noe som igjen kan skape inngang for rekruttering til radikale miljø. Her sier Øvrum[7] at en alminneliggjøring av bekymringssamtalen kan være et virkemiddel for å motvirke negativ stigmatiserende effekt.

[4] **Stempling**: "Den prosess som leder til at en person utpekes og merkes som en avviker"(Hauge,2007,s.374).
[5] **Stigmatisering:** "Man opplever seg selv som avviker og går inn i avvikerrollen"(Hauge,2007,s.374).
[6] **Marginalisering** beskriver prosesser der enkeltindivider eller grupper blir utstøtt, eller dradd mot samfunnets ytterkant(Fauske&Øya,2010,s.231)
[7] **Bjørn Øvrum**: Forelesning på Politihøyskolen 4.november 2013.

3.6 EUs Datalagringsdirektiv

Et eksempel på bruk av Datagraving og Big Data er EUs Datalagtingsdirektiv(forkortet DLD). Etter terrorangrepene i Madrid 2004 og London 2005 vedtok EU-parlamentet i 2006 å innføre et nytt rammeverk for lagring av tele- og internettopplysninger(Datatilsynet,2012b). DLD innebærer at det vil registreres hvem man kommuniserer med, på hvilket tidspunkt, hvor du befinner deg når du gjør det, samt når du er logget på Internett. Direktivet er omstridt i flere land, og har blitt kritisert for å være et urimelig inngrep i privatlivet(Knoph&Lilleholt, 2004,s.104).

Formålet med DLD er å sikre myndighetene tilgang til kommunikasjonsdata, både for å avdekke, etterforske og straffeforfølge alvorlig kriminalitet. Politiet har dermed mulighet til å gå tilbake i tid, og få tilgang på samtlige samtaler, tekstmeldinger og e-poster en person har sendt og mottatt. Dette er kunnskapsbasert informasjonsinnhenting. Gjennom kartlegging oppnår myndighetene innsikt i våre sosiale nettverk og bevegelsesmønstre. Her vil det også åpne seg mulighet for datagraving i datamaterialet. Samferdselsdepartementet ser for seg at lagringsplikten trer i kraft 1.januar 2015(Færaas,2013).

Et viktig spørsmål rundt det å samle store datamengder om hele befolkningen, er om dette samsvarer med de grunnleggende menneskerettigheter Norge har forpliktet seg til å fremme. Et kjennetegn på et fritt og åpent demokrati er en sterk offentlig debatt, rettet mot alle sider av samfunnet. Dette inkluderer balansen mellom legitime sikkerhetsinteresser og beskyttelse av privatliv. Videre kreves det demokratiske regler, og rettigheter som respekteres. En av disse rettighetene er personvern. Det bygger videre på tillitt til enkeltmennesket, der vern om personlig integritet er viktig. Enkeltmennesket har rett til å etablere det som i sosiologien kalles autonomi. Dette er et ”frirom” der makta ikke når fram, hvor man kan være herre i sitt eget liv uten tvang eller innblanding fra staten(Krange&Skogen,2003).

Uten privatliv vil det ikke være mulig for mennesker å skape et rom for selvstendige refleksjoner, uten å bli forstyrret av andre. Dette vil kunne begrense borgernes åpne meningsutveksling. På den måten vil man kunne sette begrensninger på seg selv, fordi man frykter at myndighetene skal registrere og lagre opplysningene(Datatilsynet, 2012a). Dette vil kunne skape en nedkjøling av viktige samfunnsdebatter og redusert engasjement.

De fleste traktater om menneskerettigheter inneholder bestemmelser som anerkjenner personvern som grunnleggende rettighet. Norsk personvern hviler på flere slike grunnpilarer. Den europeiske menneskerettighetskonvensjonen(EMK) ble vedtatt av Europarådet i 1950, for å beskytte menneskerettighetene og de grunnleggende friheter. EMKs artikkel 8 sier

> ”*enhver har rett til respekt for sitt privatliv og familieliv, sitt hjem og sin korrespondanse*” og
>
> ”*det skal ikke skje inngrep av offentlige myndigheter i utøvelsen av denne rettigheten unntatt når dette er(…)nødvendig(…)*”(Menneskerettighetsloven,1999).

Forpliktelsen skal oppfattes som en begrensning for statens inngripen mot enkeltmennesker. Spørsmålet er om Datalagringsdirektivet, og flere av nåtidens terrortiltak, lar seg gjennomføre om vi samtidig skal kunne ivareta denne forpliktelsen. Politiet har stilt seg positivt til å innføre direktivet, og Justisdepartementet har gått inn for å lagre data om personer i ett år(Stortinget,2011). Departementet skriver at det er lagt opp stramme rammer for bruken av DLD, og hensynet til personvernet er søkt ivaretatt ved at det foreslås strenge krav til informasjonssikkerhet og sletting.

3.7 Formell-/uformell sosial kontroll

Et sunnhetstegn på et velfungerende demokratisk samfunn er en hensiktsmessig balansegang mellom formell- og uformell sosial kontroll. Ved at vi ferdes ute er vi naturlige overvåkere av hverandre(Fauske&Øya,2010,s.236). På den måten styres og styrer vi andre via en uformell sosial kontroll som er bygget inn i det sosiale liv. I den sammenheng må vi passe på at også den formelle kontrollen, via situasjonelle overvåkingstiltak, er på et akseptabelt nivå.

Politiets datagraving er et eksempel på formell kontroll. Selv om datagraving alene kan sees på som et lite inngrep, kan den samlede mengden tiltak utgjøre en mektig sosial kontroll som er med på å frata oss personlig frihet. Lie skriver at denne formen for overvåkingskontroll er så behagelig umerket, at vi sjelden stiller spørsmål ved nødvendigheten av kontrollen vi utsettes for(2011,s.269). Denne formaliserte kontrollen(…)kan svekke forutsetningene for den uformelle kontrollen ved at folk blir passivisert(Aas,Runhovde,Strype&Bjørgo,2010,s.81).

Generelt kan det virke som overvåkingstiltak har en ”placebo-effekt” på publikum. Det skapes en psykologisk trygghetsfølelse, men tiltakene har samtidig en bivirkning med redusert personvern. Da redusert personvern er usynlig for majoriteten av befolkningen, og tilsynelatende kun får konsekvenser for kriminelle, vil den ofte oppleves som positiv av offentligheten. I så måte kan overvåkingstiltakene skape en symbolsk effekt ved å øke det Aas kaller den subjektive trygghetsfølelsen(et al.,2010,s.22) hos publikum, mens andre vil kunne oppleve frykt og redusert livskvalitet.

3.8 Lovverk

Når det gjelder datagraving i metadata for terrorforebygging vil det være overvåkingstjenesten som utfører dette, da dette er deres ansvarsområde(SNL,2009a). Overvåkingstjenesten i Norge kan overordnet sies å være tredelt(SNL,2009b): Politiets Sikkerhetstjeneste(PST), forsvarets Sikkerhet&Etterretningstjeneste(E-tjenesten) og Norsk Sikkerhetsmyndighet(NSM). Litt forenklet kan man si at PST har ansvar for alt innenfor Norges grenser, mens E-tjenesten har ansvar for alt utenfor Norges grenser. NSM skal fungere som bindeleddet mellom de to instanser, som er lovpålagt å samarbeide med hverandre[8]. Ved behov samarbeider overvåkingstjenesten med tilsvarende organer i land som Norge samarbeider med[9].

3.8.1 Politiets sikkerhetstjeneste(PST)

PST er et av politiets særorgan. De skal utføre sine forebyggende oppgaver etter Politiloven ved blant annet å innhente, bearbeide, analysere og utveksle informasjon i samsvar med fastsatte prioriteringer(PST-instruksen,2005). All virksomhet som PST bedriver skal være i samsvar med gjeldende lover, forskrifter og underordnet regelverk, herunder reglene for tvangsmiddelbruk i straffeprosesslovens fjerde del.

[8] Jamfør ”Instruks for politiets sikkerhetstjeneste” §10 og ”Instruks om samarbeidet mellom Etterretningstjenesten og Politiets sikkerhetstjeneste”
[9] Jamfør ”Instruks for politiets sikkerhetstjeneste” §11.

Den sentrale forskjellen mellom PST og det "ordinære politiet" er at PST etter politiloven §17d også kan benytte visse typer tvangsmidler i forebyggende øyemed. I 2.ledd står det:

> *"Tillatelsen kan bare gis dersom det er grunn til å tro at inngrepet vil gi opplysninger av vesentlig betydning for å kunne forebygge handlingen(…)og forholdene ellers ikke fremstår som uforholdsmessig(...)."*

Når det gjelder "datagraving" kan ikke dette alene sees på som et tvangstiltak. Dette er analytisk arbeid, og dermed mer å beregne som taktisk etterforsking. Men INNHENTINGEN av data som brukes i samband med datagraving blir noe annet. Dette kan skje i form av avlytting eller gjennom beslag, som er hjemlet i straffeprosesslovens §§170a, 203 og 216. Dette er åpenbart tvangstiltak, hvor "skjellig grunn til mistanke" kreves. Dersom konkret mistanke ikke foreligger, er lovligheten tvilsom(Knoph&Lilleholt,2004,s.103). Som et tiltak for forebygging av terrorisme kan det derfor diskuteres om PST lovlig kan gjennomføre datagraving i metadata av HELE det norske folk for å finne potensielle terrorister, med mindre det er "skjellig grunn til å mistenkeliggjøre" hele befolkningen!

4 Terrorisme og trusselnivå

Terrorisme er en gammel fiende med røtter i mange kulturer og trossamfunn. Historisk har det blitt ført av en lang rekke enkeltpersoner og grupper. Det er et kjent ordtak som sier

"En manns frihetskjemper er en annen manns terrorist."
(Nordenhaug&Engene,2008,s.14).

Dette illustrerer at terroristen av i går kan bli helten i dag, mens helten av i går kan bli terroristen i dag. I et konstant skiftende verdensbilde må vi holde tungen rett i munnen for å vite hva som er, og ikke er, terrorisme.

4.1 Nåtidens terrorbølge

For ytterligere å belyse politiets bruk av datagraving som forebyggende metode mot terrorisme, har jeg sett på nåtidens terror. Nordenhaug&Engene deler den "moderne tidens terrorisme" inn i fire terrorbølger(2008,s.21).

Vår tids terrorisme betegnes som den fjerde bølgen, og vokste frem på 1980-tallet. Bølgen skiller seg fra de foregående ved at terrorhandlingene i større grad har religiøse motiver, og da spesielt islamistiske. Et annet kjennetegn ved den fjerde terrorbølgen er at anslagene er råere og har en mer spektakulær form. Den inntreffer ofte uten forvarsel, og retter seg ofte mot sivile mål. Det er også en sterkere dyrkelse av martyrrollen. Mens den gamle terrorismen var mer beregnede og forutsigbar, drives den nye terrorismen av irrasjonelle motiver. Troen på saken gjør ikke døden til en straff, men til en belønning.

Dette er stikk i strid med det man ønsker å oppnå innenfor den relative straffeteorien(Andenæs,1996,s.13). Teorien snakker om straffens avskrekkende effekt som allmennprevensjon. En forutsetning for at trusselen om straff skal virke allmennpreventivt er rasjonalitet. Sett opp mot politirollen vil derfor trusler om straff og maktbruk ha liten innvirkning på dagens terrorist.

Her oppstår det altså en konflikt med datagraving som situasjonell forebyggingsmetode. Situasjonell forebygging er basert på at lovbryter foretar en avveining av lovbruddet ut fra rasjonelle valg(Lie,2011,s.253). Lie sier videre at teorien rundt den rasjonelle aktør gir inntrykk av å ha tro på mennesket. Mennesker som velger å begå lovbrudd gjør det av egen fri vilje, og vil utfører en ”kost-nytte-analyse” for å avgjøre om lovbruddet lønner seg(Lie,2011, s.254). Handlinger styrt av religiøse motiver og belønning etter døden samsvarer ikke med denne beskrivelsen. Teorien om den rasjonelle aktør passer dermed ikke inn i den irrasjonale terroristens beskrivelse.

4.2 Norsk trusselnivå

PST opererer ikke lenger med et nasjonalt trusselnivå i Norge. De mener det åpne demokratiske samfunnet alltid vil være sårbart, og at det ikke blir tryggere ved å øke trusselnivået(PST,2013). Trusselbildet blir isteden formidlet via årlige trusselvurderinger.

PST definerer ekstrem islamisme som den største terrortrusselen for Norge ved sin siste trusselvurdering(PST,2014). Det er flere årsaker til dette. Den norske militære deltakelsen i Afghanistan kan være årsak til at norske mål oppfattes som legitime for islamistiske ekstremister. Norske oljeselskapers økende internasjonale engasjement kan på samme måte

øke faren for at olje- og gassinfrastrukturen i Norge blir sett på som et mulig terror- og sabotasjemål. Globalisering og fattigdom har også begynt å trigge terroristhandlinger. Mennesker blir mer oppmerksom på de store forskjeller i livsstil, ressurser og rikdom som eksisterer i det globale samfunnet. Det blir stadig lettere å mislike og hate de som har mye, men ikke ønsker å dele. I tillegg står deler av Europa framfor en langvarig økonomisk krise, som kan føre til økt fattigdom. Høy migrasjon kan skape grunnlag for økte konflikter langs etniske, kulturelle, sosiale og økonomiske skillelinjer. Tilstrømningen av flyktninger og asylsøkere til Norge fra konfliktområder kan i så måte ”produsere” terrorister (Nordenhaug&Engene,2008,s.61). Dette har vært sentralt i mediebildet den siste tiden, spesielt i forbindelse med nordmenn som reiser til Syria for å støtte opprørsbevegelsen.

For å belyse den faktiske faren for å bli rammet av terrorisme har jeg undersøkt terrortallene i verden. Ifølge START(2012) sin “Global Terrorism Database” har antall terrorofre økt på verdensbasis under ”kampen mot terror” de siste ti årene, sett i forhold til gjennomsnittet de siste 42 årene(3.384 kontra 4.700 per år). Terrorofre i Vesten er for øvrig redusert 4,5 ganger i samme periode(212 kontra 46,5 per år). Årsaken til dette kan skyldes Vestens økende forebygging av terrortiltak.

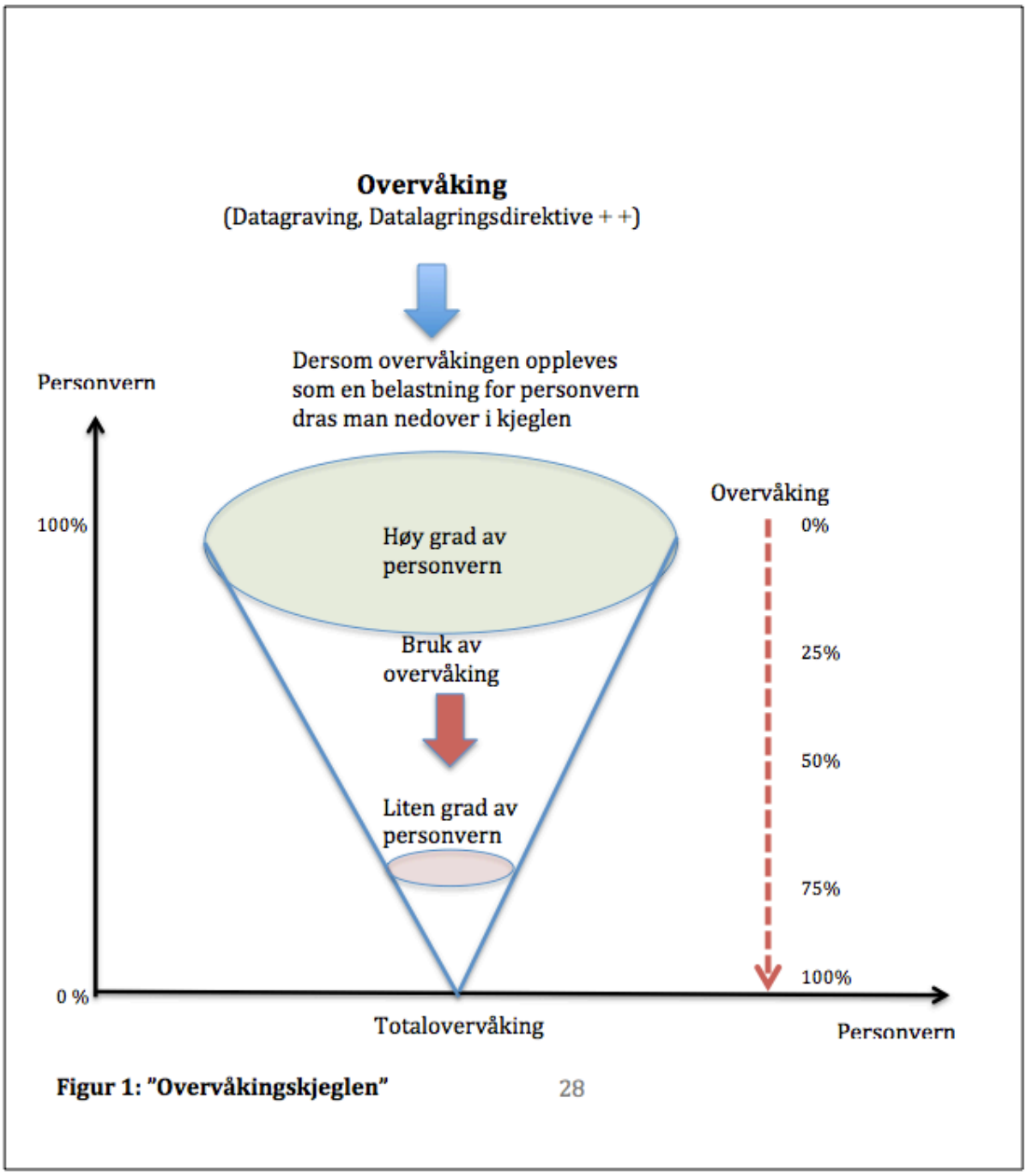
5 Datagraving versus personvern

I tidligere kapitler har jeg gitt et innblikk i hvordan datagraving i metadata kan brukes til å forebygge terrorisme. Jeg har også sett hvordan personvernet står som en grunnleggende rettighet i det norske demokratiet.

I dette kapitlet vil jeg stille disse **motpolene** opp mot hverandre, og se på hvilke negative konsekvenser datagraving kan ha for personvern.

5.1 Totalovervåking

Personvern og ”kriminalitetsbekjempelse via overvåking” er to legetime interesser som kan settes opp mot hverandre. På mange måter kan man si at personvern og overvåking har motsatt virkning på hverandre. En økning av den ene vil på mange måter redusere den andre. Dette har jeg forsøkt å illustrert via ”overvåkingskjeglen” nedenfor(figur 1).



Figur 1: "Overvåkingskjeglen" 28

Det er derfor viktig å foreta en avveining i spenningsfeltet mellom disse. Et overordnet mål må være å holde overvåkingen nede på et minimum, slik at vi alltid befinner oss øverst i kjeglen hvor det er høyest grad av personvern. Her må forholdsmessighet mellom formålet ved å bekjempe terrorisme veies opp mot redusert personvern.

Går politiet for langt i den situasjonsorienterte forebygging, risikerer man å skape et kontroll- og overvåkingssamfunn som hindrer grunnleggende verdier, som fri og anonym ferdsel i det

offentlige rom(Aas,Runhovde,Strype&Bjørgo,2010,s.81). Da vil samfunnet kunne sammenliknes med George Orwells roman ”1984”. Handlingen i denne romanen foregår i et mørkt og dystert bysamfunn, hvor “Storebror”(alias storsamfunnet) alltid ser og overvåker innbyggerne(Orwell,1949). Boka har ofte blitt brukt som en metafor på hvordan samfunnet er i ferd med å utvikle seg, og farene som har oppstått med informasjonssamfunnet.

Men der Orwell beskriver en overvåking som er påtvunget oss, har dagens samfunn godtatt utviklingen uten store protester. Kontrollen oppleves ikke som tyngende og ubehagelig, men er like total selv om den ikke merkes(Lie,2011,s.270). De fleste mennesker har en ganske blind tillit til at myndighetene alltid opptrer korrekt. Uvitende til hvilken informasjon andre kan høste av vår aktivitet på internett, har vi latt oss registrere og overvåke. Mange tenker at overvåking gjør verden tryggere, og dermed bryr de seg ikke. Da ser man bort fra hvor sensitiv personinformasjon er, og hvor mye makt den kan gi innehaveren av den. Dette gjelder spesielt når informasjon faller i gale hender. Dersom ikke lovgivningen er streng nok kan veien mot generell kommunikasjonskontroll være kort. Samtidig er det viktig at politietaten(…)handler innenfor de rammer som gjeldende rett oppstiller, ellers kan samfunnet utvikle tendenser til å bli en politistat(Nilstad&Nilsen,2004,s.87).

Hauge forklarer behovet for økt overvåking som et resultat av det industrielle samfunn(2001,s.19). Tidligere kunne mennesker identifiseres og kontrolleres gjennom sin tilhørighet til felleskapsgrupper. I dag trenger man andre kontrollmuligheter for å kunne kartlegge de grupper som kan tenkes å være en trussel mot samfunnet(Hauge,2001,s.19). Her kan man dra paralleller mot det Sahlin beskriver som ”nolltolerans som stridsredskap”, der en negativ konsekvens av for mye overvåking kan være en ”demonisering av grupperinger i samfunnet”(2001,s.100). Nulltoleransens personifisering av mulige terroristaktører vil først kunne lede til at religiøse grupperinger stemples, og deretter til at de konstrueres som fiender som skal bekjempes med ethvert lovlig middel. Sahlin skriver at dette kan føre til en undertrykkende spiral, der lengre straff og mer overvåking kreves(2001,s.102). Her kan man også dra paralleller til Christie&Bruun´s bok ”Den gode fiende”(1985), der terroristen blir en felles fiende som samler og forener befolkningen. På den måten ”glemmer” man andre samfunnsmessige problemer, noe som gir større handlingsrom og rettferdiggjør ekstraordinære kontrolltiltak.

5.2 Utglidningsprosess

Datalagringsdirektivet(DLD) er en radikal kursendring i norsk politikk. I dag er tele- og internettselskapene pålagt å slette informasjon om telefon- og internettrafikk etter fakturering. Direktivet vil innebære at selskapene nå vil være pålagt å lagre dem.

Ved hjelp av ”datagraving” i datamengden som produseres ved DLD, vil politiet ha mulighet til gå på skattejakt i dataene i håp om å finne noe av betydning. Her kan man lete etter bestemte mønstre som kan brukes til å identifisere eksempelvis terrorister.

En norsk-muslimsk mann i 20-årene, tilknyttet et bestemt religiøst miljø, som jevnlig reiser på ferie til Pakistan, kan fort havne i politiets søkelys via datagraving. Dette fordi det er ”grunn til å tro” at han under utenlandsoppholdet KAN gjennomgå en radikaliseringsprosess, som innebærer terrortrening som senere kan brukes i Norge. Etterforskere kan dermed utsette personen for andre tvangsmidler, som spaning og romavlytting. Dette fordi man gjennom datagraving har kommet fram til det som rettsvesenet må ha før man tillater dette, nemlig ”skjellig grunn til mistanke”. Problemet med en slik tilnærming er at hele befolkningen i utgangspunktet er utpekt som mistenkt FØR datagravingen. Slik beveger vi oss fra et etterforskningsprinsipp mot et overvåkingsprinsipp. Lie påpeker at vi forsøker å forutse fare ved systematisk å benytte oss av data om allerede begåtte handlinger(2011,s.270). På den måten risikerer vi å forhåndsdømme personer for handlinger som enda ikke er begått!

Vi havner i det filosof og forfatter Hammerlin kaller **”**slippery-slope-problemet”(2009,s.41), som jeg har valgt å kalle en **utglidningsprosess**: Når man først har igangsatt et system, vil det vanskelig kunne reverseres, og faren for at det vil spre seg til andre formål er stor. Det handler om grenser som flyttes. De valgene vi tar nå, kan feste seg til samfunnsstrukturen for alltid. Når man først har åpnet opp for Datalagringsdirektivet kan det bli vanskelig å stoppe eller snu. Graver sier at staten bør bekymre seg over evnen til å stå imot angrep på rettsstaten innenfra gjennom samfunnet selv og dets ordinære kanaler(2011,s.111). Dette har vi sett eksempler på ved kontrollen med overvåkingen, sier han videre. DLD vil i framtiden kunne utvides til også å omfatte innholdet i epost eller telefonsamtaler, og tidsrammen på lagring i et år vil kunne forlenges. Et lite første trinn vil lett kunne føre til en kjede av relaterte hendelser, som kulminerer i en mye betydeligere virkning: en utglidningsprosess som har kommet ut av kontroll. Nordenhaug&Engene sier at denne utviklingen kan bli svært problematisk, dersom

hvert tiltak ses isolert, og uten at man vurderer hvilke konsekvenser tiltakene samlet sett får for rettsstaten(2008,s.151).

5.3 Kritisk bruk av datagraving

Uavhengig av årsak, er terrorisme uakseptabel atferd som ikke skal få lov til å råde ukontrollert. Politiet må strekke seg langt for å beskytte sine samfunnsborgere, gjerne ved bruk av situasjonsforebyggende tiltak som datagraving. Men ikke for enhver pris! Skal vi ta vare på demokratiske verdier må vi ha gjennomtenkte lover og regler, uten smutthull, som har rettsprinsipper og personvern i høyfokus. Og disse lovene må følges, selv av overvåkingstjenester. Det betyr at eventuelle ”skjønnsrom” overvåkingstjenesten opererer i, der lovens grenser utsettes for elastisk behandling, må tettes. Vi kan ikke ha grupperinger i samfunnet som tillater seg å ha virksomhet på utsiden av loven. Dette betyr at vi må ha kontrollorganer som kan kontrollere at regler overholdes, og disse må ha full innsynsrett. Ellers blir det ”bukken som passer havresekken”, og da risikerer vi å få en ”stat i staten”.

Data-fagfeltet er endeløst, svært teknisk og uoversiktlig. Dette er ”en upløyd mark”, med mange uavklarte spørsmål det er viktig å få belyst. Et spørsmål her er om det er praktisk mulig å underlegge politi og overvåkingstjenesten god nok demokratisk kontroll, når man overvåker sanntidsdata i hele verden?

Vi må videre ha en kritisk vurdering av metadataene som brukes, og ikke bare akseptere data som sannferdige uten videre. Ikke all informasjon som eksisterer på nett har sin rot i virkeligheten. Objektivitet er svært viktig. Evnen til å plukke ut den informasjonen som er viktig og relevant er ikke lett. Lie skriver at informasjonen skaper en forutinntatthet hos den som leser det, og at utgangspunktet ofte er ensidig negativt(2011,s.272). Hun sier det derfor blir viktig at man aktivt søker annen informasjon(…)som kan supplere bildet med bredere kunnskap, og ikke bare bekrefte bildet man allerede sitter med(Lie,2011,s.273).

Til slutt må vi ha i bakhodet at regler vi lager for å beskytte samfunnet, av og til kan ha motsatt virkning. Vi må derfor ha rom for å kunne reversere og snu prosesser vi ser har uheldige konsekvenser, og vi må kunne sette begrensninger for en videreføring av slike tiltak.

Her sikter jeg spesielt til Datalagringsdirektivet. Et uavklart spørsmålet er hvor langt man kan gå i datainnhøsting og analyse, før man har en mistanke eller en sak.

Politiet kan ikke stoppe alle muligheter for at en terroristhandling kan oppstå, men kan sammen med resten av samfunnet tilstrebe å forstå mekanismene som fører til terrorisme. Deretter kan samfunnet i fellesskap forsøke å gjøre noe med disse terror-katalysatorene, slik som fattigdom, skjevfordelinger og arbeidsløshet. Det å forstå kan gjøre oss bedre rustet til å takle og håndtere, uten at vi over-responderer, og uten at vi lukker øynene for trusselen som konfronterer oss.

6 Avslutning

> *"Kampen mot terrorisme er dypest sett en kamp om verdier. Og vår innsats mot terror vil bare lykkes dersom kampen føres i full overensstemmelse med rettsstatens prinsipper og de universelle menneskerettigheter*".

Ordene ovenfor ble uttalt av utenriksminister Støre(Utenriksdepartementet,2006), og illustrerer essensen i det jeg har kommet fram til. Jeg har i oppgaven prøvd å illustrere at det eksisterer en frykt for terrorisme i samfunnet, men at denne frykten ikke står i samsvar med sannsynligheten for å bli rammet. Likevel står befolkningen ovenfor omfattende situasjonelle forebyggingstiltak, som eksempelvis Datalagringsdirektivet. Dette er tiltak som går på bekostning av personvern og privatliv, og som lett lar seg videreutvikle i det jeg har kalt en utglidningsprosess. Små endringer kan flytte grenser og verdier ytterligere.

Blir vi overvåket via generell datagraving eller ikke? Jeg har vist til et norsk lovverk, med en intensjon om å beskytte befolkningen mot unødvendig datagraving. Overvåkingstjenesten forteller lite om sin virksomhet. Det eksisterer derfor usikkerhet rundt eksisterende datagraving i Norge i dag. Denne usikkerheten kan gå på bekostning av publikums tillit til politiet.

I Norge står personvernet sterkt sammenlignet med mange andre land, og er et av de landene i verden hvor man har størst tillit til staten(Utheim,2013). Demokratiske nasjoner, med Norge i spissen, må veie opp kostnadene i form av tapt frihet, mot gevinsten av å kue terrorisme.

Samtidig må man innrømme at det å ofre frihet kan bli sett på som å gi terrorisme seieren den søker: nemlig ødeleggelse av demokratiske systemer. Kostnaden av å vinne kampene mot terrorisme kan dermed bli stor.

I statsminister Stoltenbergs tale ved 2.års markeringen for 22.juli-terroren nevnte han flere tiltak som har blitt gjennomført etter 2011. Han sa videre:

> *"Like viktig er det å vokte verdiene som ble angrepet 22.juli: humanitet, mangfold, solidaritet, vårt åpne og tillitsfulle fellesskap(…).Vi må aldri oppgi våre verdier i møtet med terroren. Svaret på vold er mer åpenhet*".

Det blir derfor viktig å ivareta våre demokratiets grunnprinsipper i tiden som kommer, samtidig som politiet og samfunnet får det lovverk og de verktøy som er nødvendig for å ivareta et trygt demokrati. Det er en skjør balansegang mellom Datalagringsdirektivet, datagraving og ivaretagelse av personvernet. Ny teknologi må derfor være basert på veltenkte vurderinger, og lover som regulerer både dagens og fremtidig bruk. Det er ikke sikkert fullstendig rettsikkerhet og terroristbekjempelse er forenelig. Datalagringsdirektivet kan være et isfjell som venter på Titanic!

7 Litteraturliste

Aas, G., Runhovde, S., Strype, J. & Bjørgo, T. (Red.).(2010). *Trygghet i det offentlige rom: I åtte norske kommuner og bydeler.* (PHS Forskning, 2010:7). Oslo: Politihøyskolen.

Aadland, E. (2011). *Eg ser på deg.…: Vitenskapsteori i helse- og sosialfag* (3.utg.). Oslo: Universitetsforlaget.

Andenæs, J. (1996). *Straffen som problem*. Exil Forlag AS.

Christoffersen S.A. (2011). *Profesjonsetikk*. Oslo: Universitetsforlaget AS.

Bjørgo, T. (2011). *Forebygging av terrorisme og annen kriminalitet*. Politihøyskolen.

Bleikelia, M., Færaas, A., Johansen, P. (2013, 4.august). *Nytt norsk overvåkingsprogram åpner for mer overvålking*. Hentet 8.juli 2013 fra http://www.aftenposten.no/nyheter/iriks/Forst-i-2015-skal-din-e-post--og-telefoninfo-lagres-7185521.html#comment-876813007)

Bruun, K. & Christie, N. (1985) *Den gode fiende : narkotikapolitikk i Norden*. Oslo : Universitetsforlaget.

Dalland, O. (2012). *Metode og oppgaveskriving for studenter*. Oslo: Gyldendal akademisk.

Datatilsynet. (2012a, 11.mai). *Big Data er deg*. Hentet 1.juli 2013 fra http://www.datatilsynet.no/verktoy-skjema/Publikasjoner/Analyser-utredninger/Big-data-er-deg/

Datatilsynet. (2012b, 2.august). *Datalagringsdirektivet(DLD)*. Hentet 8.juli 2013 fra http://www.datatilsynet.no/Teknologi/Datalagringsdirektivet/Om-datalagringsdirektivet/

Fauske, H. & Øya T. (2010). *Oppvekst i Norge* (2.rev.utg.) Oslo: Abstrakt.

Frønes, I. (2011). ”Den digitale barndommen”. I: ”*Moderne barndom* (3.utg.) Oslo: Cappelen Damm Akademiske.

Færaas, A. (2013, 26.april). *Først I 2015 skal din e-post- og telefoninfo lagres*. Hentet 8.juli 2013 fra http://www.aftenposten.no/nyheter/iriks/Nytt-norsk-spionprogram-apner-for-mer-overvaking-7270314.html#.Uqo8uSgRwpg

Graver, H.P. (2011). *Hva er rett?* Oslo: Universitetsforlaget.

Hammerlin, J. (2009). *Terrorindustrien*. Forlaget Manifest AS.

Hauge, R. (2001). *Kriminalitetens årsaker* (2.utg.). Oslo: Universitetsforlaget.

Hauge, R. (2007). Stempling og stigmatisering. I L. Finstad & C. Høygård (Red.), *Kriminologi* (4.utg). Oslo: Pax.Oslo

Hopperstad, M. & Johnsen, N. (2013, 3.november). *30 unge innkalt til bekymringssamtaler – frykter ekstremisme*. Hentet fra http://www.vg.no/nyheter/innenriks/30-unge-innkalt-til-bekymringssamtaler-frykter-ekstremisme/a/10144689/

Knoph, R. & Lilleholt, K. (2004) *Knophs oversikt over Norges rett*. Oslo: Universitetsforlaget.

Krange, O. & Skogen, K. (2003). Skudd i løse lufta? Unge jegere og rovdyrpolitikken. I: F. Engelstad & G. Ødegård (Red.), *Ungdom, makt og mening*. Oslo: Gyldendal akademisk.

Lie, E. (2011). *I forkant. Kriminalforebyggende politiarbeid*. Gyldendal Norsk Forlag AS.

Myhrer, T-G. (2011). *Vern eller hindrer?: Taushetsplikt i det kriminalforebyggende samarbeid mellom etatene.* Oslo: Politihøyskolen.

Meld.St. 21 (2012-2013). *Terrorberedskap. Oppfølging av NOU 2012: 14 Rapport fra 22.juli-kommisjonen*. Hentet fra http://www.regjeringen.no/nb/dep/jd/dok/regpubl/stmeld/2012-2013/meld-st-21-20122013.html?id=718216

Menneskerettighetsloven. (1999). *Lov om styrking av menneskerettighetenes stilling i norsk rett av 21.mai 1999*. Hentet 16.oktober 2013 fra http://www.lovdata.no/all/hl-19990521-030.html

National Consortium for the **S**tudy of **T**errorism **a**nd **R**esponses to **T**errorism (START). (2012). *Global Terrorism Database [globalterrorismdb_1012dist.xlsx]*. Retrieved 12.juli 2013 from http://www.start.umd.edu/gtd

Nilstad, M. & Nilsen, J.R. 2004). *Publikumsrettet politiarbeid: Generell del*. Nesbru: Vett & Viten.

Nordenhaug, I. & Engene, J. O. (2008). *Norge i kamp mot terrorisme*. Universitetsforlaget.

NOU 2012:14. (2012). *Rapport fra 22.juli-kommisjonen*. Hentet fra http://www.regjeringen.no/nb/dep/smk/dok/nou-er/2012/nou-2012-14.html?id=697260

NOU 2013:9. (2013). *Ett politi – rustet til å møte fremtidens utfordringer*. Hentet fra http://www.regjeringen.no/nb/dep/jd/dok/nouer/2013/nou-2013-9.html?id=730815

Politidirektoratet. (2011). *VEILEDER for politiets bekymringssamtale*. Allkopi.

Politiloven. (1995). *Politiloven av 1.oktober 1995*. Hentet 28.06.2013 fra http://www.lovdata.no/all/nl-19950804-053.html

PST. (2013, 15.februar). *Terrortrusselen og nasjonalt nivå.* Hentet 19. Juli 2013 fra http://www.pst.no/blogg/trusselniva/

PST. (2014, 4.mars). *Åpen trusselvurdering 2014.* Hentet 25. mars 2014 fra http://www.pst.no/media/67044/PSTs_tv2014.pdf

PST-instruksen. (2005). *Instruks for Politiets sikkerhetstjeneste av 19.august 2005*. Hentet 1.august 2013 fra http://www.lovdata.no/cgi-wift/ldles?doc=/sf/sf/sf-20050819-0920.htm

Sahlin, I. (2001). Nulltoleransens stadsbild. I J. F. Pacheco (Red.), *Stadskultur*. Lund: Department of Sociology, Lunds universitet.

SNL. (2009a, 14.februar). *Overvåkingstjeneste*. Hentet 16.oktober 2013 fra http://snl.no/.versions/list/overvåkingstjeneste

SNL. (2009b, 14.februar). *De hemmelige tjenester*. Hentet 16.oktober 2013 fra http://snl.no/de_hemmelige_tjenester

St.meld. nr.61 (2001-2002). *Om lov om endringer i straffeloven og straffeprosessloven mv*. Hentet fra http://www.regjeringen.no/nb/dep/jd/dok/regpubl/otprp/20012002/otprp-nr-61-2001-2002-.html?id=168459

Stortinget. (2011, 30.mars). *Innstilling og datalagringsdirektivet. 275L(2010-2011).* Hentet 8.juli 2013 fra http://www.stortinget.no/no/Saker-og-publikasjoner/Publikasjoner/Innstillinger/Stortinget/2010-2011/inns-201011-275/?lvl=0

Utenriksdepartementet. (2006). *Utenrikspolitisk strategi for bekjempelse av internasjonal terrorisme* (Publikasjonskode: E-803 B). Hentet fra http://www.regjeringen.no/upload/kilde/ud/pla/2006/0005/ddd/pdfv/291572-terrorstrategi_nor.pdf

Utheim, E. (2013, 23.juli). *Snowden ga kundeboom for norsk nettsky-firma*. Hentet fra http://e24.no/digital/snowden-saken-ga-kundeboom-for-norsk-nettsky/21106285

Vestrum A. (2013, 07.juni). *Obama forsvarer overvåking av telefon og nett*. Hentet fra http://www.aftenposten.no/nyheter/uriks/Obama-forsvarer-overvaking-av-telefon-og-nett-7224484.html#.Uc2v6OCPcpg

Selvvalgt pensum:

Nordenhaug, I. & Engene, J. O. (2008). *Norge i kamp mot terrorisme*. Universitetsforlaget. (s.11-153)

Hammerlin, J. (2009). *Terrorindustrien*. Forlaget Manifest AS. (s.44-59, 117-155, 195-235)

Bjørgo, T. (2011). *Forebygging av terrorisme og annen kriminalitet.* Politihøyskolen. (s.15-50)