PH.D.-AFHANDLING

I spændingsfeltet mellem informationel privathed og offentlig sikkerhed

- Statens overvågning af big data anvendt i sikkerhedsteknologi

Hanne Bjerre Cowling
September, 2015

I spændingsfeltet mellem informationel privathed og offentlig sikkerhed

- Statens overvågning af big data anvendt i sikkerhedsteknologi

The tension between informational privacy and public security

- Governmental surveillance of data used in security technology

Ph.d.-afhandling indleveret ved
Institut for Design og Kommunikation
Det Humanistiske Fakultet
Syddansk Universitet

Ph.d.-vejleder: lektor Anne Gerdes

Afhandlingens omfang: 702.235 anslag svarende til 293 normalsider.

Grafisk arbejde: Alison Elizabeth Barracluff/Print: Print & Sign, Syddansk Universitet/Forsidebillede: Colourbox.com

FORORD OG TAKSIGELSER

I 2009 blev jeg for første gang introduceret til it-etik i kraft af mit studie, Humanistisk Informationsvidenskab på Syddansk Universitet. Det var også startskuddet til en stor interesse for et genstandsfelt, der er i konstant udvikling. Siden 2009 har jeg fulgt denne faglige interesse på studiet, når det har været mig muligt.

Min primære it-etiske interesse har været privathed, og derfor blev omdrejningspunktet for mit speciale netop også privathed – dog belyst i forhold til data i sundhedssektoren.

I efteråret 2012 startede jeg mit ph.d.-forløb, hvor jeg var så heldig igen at få muligheden for at undersøge privathed. Denne gang i langt flere detaljer, hvilket har åbnet mine øjne for den enorme kompleksitet, der omgærder privathed. Privathed er på én gang svært håndgribeligt og på samme tid har privathed (eller mangel herpå) betydelig indvirkning i mange aspekter af livet. Privathed bliver i den verden, vi lever i i dag udfordret, og er i nogle tilfælde også kommet under alvorligt pres som følge af de teknologiske muligheder, der eksisterer.

I nærværende afhandling er privathed undersøgt i lyset af staters overvågning af *big data,* med henblik på at opretholde den offentlige sikkerhed. Det er en problemstilling, der har massiv bevågenhed i den tid, vi befinder os i – ikke mindst grundet Edward Snowden, der i sommeren 2013 lækkede fortrolige dokumenter om NSA's overvågning af individer. Også EU's Logningsdirektiv har fået stor opmærksomhed både før og efter, at dette blev erklæret ugyldigt i menneskerettighedsdomstolen i april 2014.

Den offentlige sikkerhed bliver brugt som et argument for, at stater kan tillade sig at udføre massiv overvågning af individers data. Det er trods alt til det fælles bedste. I afhandlingen udfordrer jeg antagelsen om, at offentlig sikkerhed bør have fortrinsret i forhold til informationel privathed, som det i nogle tilfælde kommer til udtryk i staters praksis. Det påpeges også i afhandlingen, at mangel på informationel privathed ikke kun er et tab for det enkelte individ, men tillige kan betragtes som et tab for både staten og samfundet. Godtages argumentationen for, at offentlig sikkerhed og informationel privathed er to værdier, der beg-

ge er væsentlige for stat, samfund og individ, er det hensigtsmæssigt at ville realisere disse værdier i teknologi. Slutteligt i afhandlingen vurderes forskellige tilgange til at realisere værdier i teknologi.

Afhandlingsprocessen har været lærerig og udfordrende. En række personer været medvirkende til, at jeg nu har indleveret min afhandling.

Først og fremmest vil jeg gerne sige stor tak til min ph.d.-vejleder, lektor Anne Gerdes. Anne har altid stillet sig til rådighed til læsning af kapitler og diskussioner af afhandlingen. Anne har udfordret mig i stadig stigende grad under ph.d.-forløbet, hvilket har været grundlaget for en meget lærerig proces. Også tak til Anne for tidligt i mit forløb at skabe kontakt til det amerikanske forskningscenter, *Research Center on Computing and Society* ledet af professor Terry Ward Bynum. Jeg besøgte forskningscenteret som en del af mit miljøskifte i starten af 2013. Terry, der er en af det it-etiske forskningsfelts grundlæggere, tog sig masser af tid til at snakke om min afhandling og dele ud af sin imponerende erfaring. Derudover har Klaus Robering, professor på institut for Design og kommunikation bistået med sparring og vejledning på dele af afhandlingen. Det har været en betydningsfuld hjælp, der har givet nye perspektiver til min skriveproces.

Tak til familie og venner, der har lagt øre til både mine frustrationer og glæder over arbejdet med afhandlingen. Særligt min mor har lagt øre til meget og har altid stået klar med masser af opmuntring - mange tak. Ligeledes vil jeg gerne takke mine søskende, Lene og Lars, der begge har været gode sparringspartnere vedrørende de af afhandlingens emner, som de i kraft af deres studier har kendskab til. En stor tak skal min far have for at have læst korrektur på afhandlingen.

Tak til min mand Simon Cowling, som jeg har brugt meget tid med i Australien, imens jeg har skrevet på min ph.d.-afhandling, for altid at være villig til at diskutere min afhandling og lytte til frustrationer og glæder undervejs i projektet.

Hanne Bjerre Cowling
Kolding, 2015

RESUME

Stater indsamler og overvåger massive mængder *big data* om individer med det formål at opretholde eller øge den offentlige sikkerhed. Data indsamlet med hjemmel i EU's Logningsdirektiv, det amerikanske National Security Agencys overvågning af metadata om telekommunikation og indhold i chats på sociale medier og i e-mails er alle eksempler herpå. Overvågning af *big data* kan betyde, at individers informationelle privathed sættes under pres.

Kernen i afhandlingens it-etiske problemstilling er den spænding, der findes mellem værdierne informationel privathed og offentlig sikkerhed, når stater overvåger individer. På baggrund af en teoretisk diskussion af nævnte værdier argumenteres der for, at informationel privathed og offentlig sikkerhed begge har betydning for staten, samfundet og individet.

Overvågning og konsekvenserne heraf diskuteres primært med en sociologisk tilgang, hvorved overvågningens kompleksitet illustreres. Ydermere diskuteres implikationer af overvågning, hvor det primære fokus er overvågning af data, såkaldte *dataveillance.*

Informationel privathed belyses og diskuteres med afsæt i filosofisk litteratur herom. Det gøres gældende, at privathed er en betingelse for intrinsiske værdier som autonomi, integritet og interpersonelle relationer. Ydermere demonstreres det, hvorledes informationel privathed har betydning for det liberale demokrati og samfundet som helhed. Retskilder, der navnlig omhandler databeskyttelse i EU, præsenteres og diskuteres med henblik på at afklare den nuværende juridiske beskyttelse. I forlængelse heraf fremstilles en argumentation for, hvorfor etiske overvejelser i forbindelse med databeskyttelse stadig har deres berettigelse.

Offentlig sikkerhed og den ontologiske relation mellem stat og individ behandles med udgangspunkt i politisk filosofi. På baggrund af beskrivelser af informationel privathed og offentlig sikkerhed sandsynliggøres det, at en stat ikke alene skader individer ved at udføre massiv overvågning; staten skader også samfundet og statskonstruktionen som helhed. Antagelsen om, at offentlig sikkerhed

bør have fortrinsret i forhold til informationel privathed i sikkerhedsteknologi, som det i nogle tilfælde kommer til udtryk i staters praksis, udfordres således i afhandlingen.

Den spænding, der eksisterer mellem informationel privathed og offentlig sikkerhed manifesterer sig også i sikkerhedsteknologier, som stater kan gøre brug af. Som afsæt for diskussion og til illustration af teoretiske pointer inddrages tre sikkerhedsteknologier som scenarier, hvorved mulig brug af sikkerhedsteknologi eksemplificeres. Scenarierne illustrerer sikkerhedsteknologier, der kan anvendes med strategisk, taktisk eller operationelt sigte med henblik på at nedsætte organiseret kriminalitet eller terror.

Med et pragmatisk afsæt diskuteres og vurderes det, hvorvidt to forskellige værdibaserede designtilgange, *Value Sensitive Design* (VSD) og *Privacy by Design* (PbD), er anvendelige med henblik på at realisere værdierne informationel privathed og offentlig sikkerhed i sikkerhedsteknologi. Designtilgangene udspringer fra enslydende grundantagelser om, at menneskelige værdier skal addresseres igennem hele designprocessen fra start til slut. Det vurderes, at såvel VSD som PbD er egnede strategier til at realisere de nævnte værdier. Det pointeres dog, at der er en række grundlæggende problemstillinger ved begge tilgange, og at disse begge bør udvikles yderligere.

SUMMARY

Governments collect and surveil a significant amount of big data pertaining to individuals in order to sustain or increase public security. Examples of this include: data collected under the European Data Retention Directive, the American National Security Agency's surveillance of telecommunication metadata and content in chats on social media. Surveillance of big data can lead to infringement on individuals' privacy.

The core of the thesis' IT-ethical problem is the tension between the values of informational privacy and public security, when states surveil individuals. Based on a theoretical discussion of the aforementioned values, arguments will be made for informational privacy and public security; both are important to the state, society and the individual.

Surveillance and its implication are primarily discussed with a sociological approach, by which the complexity of surveillance will be illustrated. Furthermore, the implications of surveillance will be discussed with a primary focus on surveillance of data, so called *dataveillance*.

Informational privacy will be discussed setting out from philosophical literature. It is claimed that privacy is a condition of intrinsic values, such as autonomy, integrity and interpersonal relations. Furthermore, it will be demonstrated how informational privacy is affecting the liberal democracy and society as a whole. Sources of law concerning data protection (primarily in the EU) are presented and discussed in order to clarify the current legal protection framework. By extension, an argument is made for ethical justification remaining valid as opposed to considerations related to data protection.

Public security and the ontological relationship between the state and the individual is treated on the basis of political philosophy. In light of the above, the positions of the values of informational privacy and public safety are investigated. It is proposed that if a state conducts surveillance program on individuals, the state is not only harming individuals, but also harming society and the state itself. The thesis challenges the assumption that public security should have pri-

ority over informational privacy in security technology, which in some cases is reflected in current national practices.

The tension that exists between informational privacy and public security is also manifested in terms of security technologies. As a starting point for discussion, and to illustrate the theoretical arguments involved, three security technology scenarios that exemplify the use of security technology are presented. The scenarios illustrate three different security technologies that can be used with strategic, tactical or operational orientation with the aim of reducing organized crime or terrorism.

It discussed and evaluated whether two different value-based design approaches, *Value Sensitive Design* (VSD) and *Privacy by Design* (PBD) is useful in order to reduce the tension between public security and informational privacy in security technology used by the state. Both design approaches are based on a basic assumption that human values must be treated proactively and that values should be addressed through the design process from start to finish. It is estimated that well VSD as PBD can be useful as strategies to realise the values of informational privacy and public security in security technology. It is emphasized, however, that there are a number of problems with both approaches and that they need further development.

INDHOLDSFORTEGNELSE

1. PROBLEMSTILLING I AFHANDLINGEN OG BAGGRUND

1. PROBLEMSTILLING I AFHANDLINGEN OG BAGGRUND

I afhandlingen vil den spænding, der eksisterer mellem informationel privathed[1] og offentlig sikkerhed, når udvalgte sikkerhedsteknologier anvendes af staten, blive belyst, diskuteret og vurderet.

Stater indsamler og overvåger i dag data om individer (Greenwald, 2014; Lovbekendtgørelse nr. 988 af 28. september 2006; Lovbekendtgørelse nr. 660 af 19. juni 2014; Regeringen, 2015). Nogle af de indsamlede data kan karakteriseres som såkaldt big data. Big data kan helt overordnet siges at henvise til det kæmpe hav af strukturerede og ustrukturerede data i forskellige formater og fra forskellige kilder, vi i dag har til rådighed (Craig & Ludloff, 2011, s. 4; Floridi, 2012; Mayer-Schönberger & Cukier, 2013). Formålet med at indsamle data er at opretholde eller øge den offentlige sikkerhed. Med offentlig sikkerhed menes sikkerhed for både staten og det enkelte individ (Aquilina, 2010; Liotta, 2002; Owen, 2004; United Nations Development Programme, 1994). Et eksempel på indsamling af data, hvor formålet er at øge sikkerheden, er Logningsbekendtgørelsen, hvori det er foreskrevet, at bestemte metadata om internet- og telekommunikation skal logges (Lovbekendtgørelse nr. 988 af 28. september 2006; Lovbekendtgørelse nr. 660 af 19. juni 2014). Det amerikanske National Security Agencys (herefter blot NSA) overvågning af metadata om telekommunikation og indhold i chats på sociale medier og i e-mails foretages også med det formål at øge offentlig sikkerhed (Greenwald, 2014).

Til trods for at overvågning af data finder sted med det formål at opretholde eller øge offentlig sikkerhed, er det imidlertid ikke uproblematisk at udføre overvågning af data, såkaldt dataveillance[2] (Clarke, 1988). En række problematiske konsekvenser er knyttet til overvågning af individers data. Der kan

[1] Informationel privathed kan overordnet karakteriseres som privathed, der knytter sig til data og/eller information.

[2] "Dataveillance" er en sammentrækning af "data" og "surveillance". Jeg vil blot henvise til dette som "dataveillance" i nærværende afhandling.

være tale om, at individers informationelle privathed sættes under pres på forskellig vis.

At tillade individer at opretholde privathed kan begrundes med, at privathed er betingelse for at kunne bevare forskellige typer af sociale relationer til andre mennesker (Rachels, 1984)[3], at privathed er en forudsætning for intimitet (Gerstein, 1984a)[4], og at privathed giver mulighed for at kunne trække sig tilbage (Benn, 1984)[5]. Mangel på privathed kan omvendt betyde, at disse individer ikke tør tænke frit og dermed ender som ensrettede personer (Clarke, 1988, s. 508; Foucault, 1995, s. 181; Peissl, 2003, s. 22; Reiman, 1995, s. 40-42)[6]. Nogle hævder, at kontrol med information om en selv er en forudsætning for, at man kan tale om privathed (Fried, 1984)[7]. Andre mener, at begrænset informationskontrol er tilstrækkeligt (Reiman, 1995).

Hvis individer ensrettes, har det ikke kun betydning for det enkelte individ. Der kan argumenteres for, at det kan have implikationer for staten og samfundet som helhed (Gavison, 1984; Regan, 1995; Regan, 2002)[8]. En nødvendig forudsætning for et velfungerende demokrati er det frie individ, der tør tænke sine egne tanker (Gavison, 1984). Tillader man ikke frie tanker og forskellighed, kan man risikere, at hele samfundets udvikling stagnerer (Peissl, 2003, s. 22; van Loenen, Groetelaers, Zevenbergen, & de Jong, 2007, s. 146).

Kernen i den problemstilling, der skitseres ovenfor, er spændingen mellem værdierne informationel privathed og offentlig sikkerhed. Informationel privathed er ofte opfattet som en instrumentel værdi, der knytter sig til individet (Fried, 1984; Gerstein, 1984a; Kupfer, 1987; Rachels, 1984; Reiman, 1984;

[3] Originalkilden blev publiceret første gang i 1975

[4] Originalkilden blev publiceret første gang i 1978.

[5] Originalkilden blev publiceret første gang i 1971.

[6] Foucualt: Originalkilden blev publiceret første gang i 1975.

[7] Originalkilden blev publiceret første gang i 1968

[8] Gavison: Originalkilden blev publiceret første gang i 1980.

Warren & Brandeis, 1984)[9, 10]. Offentlig sikkerhed er ligeledes en instrumentel værdi, der dog fejlagtigt kan opfattes som væsentlig mere værdifuld end privathed, idet offentlig sikkerhed anses for at være et gode for både stat og individ. Denne betoning af offentlig sikkerhed kommer til udtryk i såvel retskilder (Europa-parlamentet og rådets direktiv, 1995, s. art. 13, Undtagelser og begrænsninger; Folketingets EU-oplysning, art. 8, stk 1 og 2) som de politiske beslutninger, der træffes om at overvåge individer med henblik på at opnå offentlig sikkerhed (Department of Homeland Security, 2012; Lovbekendtgørelse nr. 988 af 28. september 2006; Lovbekendtgørelse nr. 660 af 19. juni 2014). Måden, hvorpå spændingen mellem informationel privathed og offentlig sikkerhed opfattes, manifesterer sig også i forhold til sikkerhedsteknologier. I afhandlingen belyses tre udvalgte sikkerhedsteknologier, og det diskuteres i den forbindelse, hvordan privathed sættes under pres.

Der findes forskellige tilgange til, hvordan man kan realisere værdier i teknologi. I afhandlingen behandles henholdsvis *Value Sensitive Design* (herefter blot VSD) (Friedman & Kahn, 2003; Friedman, Kahn, & Borning, 2006) og *Privacy by Design* (herefter blot PbD) (Cavoukian, 2011), der begge tager afsæt i en grundlæggende antagelse om, at menneskelige værdier skal behandles proaktivt i forhold til teknologi, og at værdier endvidere skal behandles igennem hele designprocessen fra start til slut. Ideen er endvidere, at bestemte værdier kan realiseres i teknologi, hvilket enten vil understøtte eller hindre bestemt brug af teknologi. Dette skal dog ses i samspil med den eller de personer, der anvender en given teknologi, idet den person også vil have indflydelse herpå (Cavoukian, 2011; Friedman, Kahn, & Borning, 2006). Der er således tale om et interaktionsperspektiv på teknologi og individer. Det vil blive diskuteret, hvordan henholdsvis VSD og PbD kan anvendes til at realisere værdierne informationel privathed og offentlig sikkerhed i sikkerhedsteknologi.

[9] Reiman: Originalkilden blev publiceret første gang i 1976.

[10] Warren og Brandies: Originalkilden blev publiceret første gang i 1890.

I ovenstående er konturerne tegnet af den problemstilling, som jeg i afhandlingen søger at belyse og vurdere i flere detaljer. Jeg udfordrer i afhandlingen antagelsen om, at offentlig sikkerhed bør have fortrinsret i forhold til informationel privathed i sikkerhedsteknologi, som det i nogle tilfælde kommer til udtryk i staters praksis. Der argumenteres for, at informationel privathed og offentlig sikkerhed begge er værdier, der har betydning for staten, samfundet og individet. Det betyder også, at en stat ikke alene skader individer ved at udføre massiv overvågning; staten skader også samfundet og statskonstruktionen som helhed. På baggrund af en teoretisk gennemgang og diskussion af værdierne informationel privathed og offentlig sikkerhed demonstreres det i afhandlingen, at det er problematisk at udvikle sikkerhedsteknologier, der ikke respekterer individets ret til informationel privathed.

Ovenstående kan betragtes som et kort oplæg til afhandlingens formål, der er at undersøge spændingen mellem privathed og offentlig sikkerhed, når sikkerhedsteknologier anvendes af staten eller offentlige institutioner. Ydermere vurderes det, om udvalgte værdibaserede designtilgange kan anvendes til at realisere værdier i teknologi.

I nærværende kapitel vil jeg udfolde ovenstående yderligere sammen med en udvidet introduktion til formålet med afhandlingen og en præsentation af afhandlingens centrale genstandsfelter. I det efterfølgende kapitel 2., *Afhandlingens fundament og struktur,* findes en diskussion af, hvorledes det it-etiske aspekt i afhandlingen kommer til udtryk. Ydermere præsenteres det, hvordan afhandlingen positionerer sig i forhold til anden forskning. I slutningen af afhandlingens andet kapitel præsenteres en læsevejledning for de enkelte kapitler.

1.1. SIKKERHEDSPOLITISKE TILTAG EFTER 11. SEPTEMBER 2001 I USA OG EU

Bevidstheden om, at offentlig sikkerhed er vigtig og samtidig ikke skal tages for givet, blev for alvor slået fast den 11. september 2001 (herefter blot 11/9 2001), hvor terrorangrebet på Manhattan fandt sted (Peissl, 2003, s. 1). Efter denne dato er der sket en oprustning af den overvågning og de juridiske mid-

ler, der anvendes med henblik på at opretholde den offentlige sikkerhed (Peissl, 2003; Raguse, Meints, Langfeldt, & Peissl, 2008; Solove, 2007, s. 745).

Mere konkret blev konsekvensen af 11/9 2001 og senere også terrorangrebene i Madrid marts 2004, London juli 2005, Paris januar 2015 og København februar 2015, at en række lande og sammenslutninger iværksatte forskellige sikkerhedspolitiske tiltag, hvilket vil blive udfoldet i nedenstående. Her vil tillige blive inddraget nogle konkrete eksempler på dataindsamling med henblik på opretholdelse af offentlig sikkerhed.

I USA betød 11/9 2001 konkret, at man etablerede det såkaldte Department of Homeland Security, der officielt åbnede 1. marts 2003, og hvis primære formål er terrorbekæmpelse og terrorbeskyttelse i USA jævnfør den amerikanske "Homeland Security Act of 2002" (Department of Homeland Security, 2012).

At den amerikanske stat indsamler, behandler og overvåger data, blev for alvor slået fast og kendt i hele verden den 6. juni 2013, da avisen The Guardian på baggrund af oplysninger fra Edward Snowden, en tidligere kontraktansat hos det statslige organ NSA, afslørede detaljer om den overvågning, der udøves af den amerikanske stat. Afsløringerne viste, at NSA ikke alene indsamler metadata om samtlige telefonopkald foretaget i USA, men også telefonforbindelser mellem USA og udlandet etableret af teleselskabet Verizon, der er USA's største teleudbyder (Greenwald, 6. juni, 2013). Den 31. juli kunne The Guardian i kraft af Snowdens oplysninger afsløre NSA's brug af XKeyscore, der er en sikkerhedsteknologi, hvis formål er at omdanne data fra nettet til viden. Snowden har til The Guardian udtalt, at han fra sit skrivebord kunne: "[...] "wiretap anyone, from you or your accountant, to a federal judge or even the president, if I had a personal email"." (Greenwald, 31. juli, 2013). Konkret påstod Snowden, at en analytiker med XKeyscore eksempelvis ville have muligheden for at se IP-adresser på alle personer fra et givent land, der har besøgt et bestemt website (Greenwald, 31. juli, 2013). Det såkaldte DNI Presenter, der også er en del af XKeyscore, kunne bruges til at tilgå og læse gemte e-mails og beskeder på sociale medier, eksempelvis Facebooks chat. I kølvandet på afsløringerne af XKeyscore bemærkede NSA i en udtalelse til The Guardian, at:

””These types of programs allow us to collect the information that enables us to perform our missions successfully – to defend the nation and to protect US and allied troops abroad."” (Greenwald, 31. juli, 2013). Formålet med den omfattende overvågning begrundes således med henvisning til det, som i afhandlingen falder under betegnelsen offentlig sikkerhed.

Overvågning og udveksling af data foregår også i Den Europæiske Union (herefter blot EU). Her har man gjort udveksling af data mellem medlemslandenes efterretningstjenester væsentligt nemmere (Peissl, 2003, s. 20).

I EU har man i 2002 vedtaget en ny, fælles definition[11] af begrebet terrorisme, hvilket indebærer, at alle relevante, terrorrelaterede data fra de enkelte med-

[11] EU's fælles definition af terror siger, at: "[...] forsætlige handlinger, således som de er defineret som lovovertrædelser i national lovgivning, der i kraft af deres karakter eller den sammenhæng, hvori de begås, kan tilføje et land eller en international organisation alvorlig skade, betragtes som terrorhandlinger, når de begås med det formål:

– alvorligt at intimidere en befolkning, eller

– uretmæssigt at tvinge offentlige myndigheder eller en international organisation til at foretage eller til at undlade at foretage en handling, eller

– alvorligt at destabilisere eller ødelægge et lands eller en international organisations grundlæggende politiske, forfatningsmæssige, økonomiske eller samfundsmæssige strukturer:

a) legemsangreb, der kan have døden til følge

b) alvorlige overgreb mod en persons fysiske integritet

c) bortførsel eller gidseltagning

d) massive ødelæggelser af et regeringsanlæg eller et offentligt anlæg, et transportsystem, en infrastruktur, herundet et edb-system, en fast platformpå kontinalsoklen, et offentligt sted eller en privat ejendom, der kan bringe menneskeliv ifare eller forårsage betydelige økonomiske tab

e) kapring af luftfartøjer, skibe eller andre kollektive transportmidler eller godstransportmidler

f) fremstilling, besiddelse, erhvervelse, transport eller levering eller brug af skydevåben, sprængstoffer, kernevåben, biologiske og kemiske våben samt, for så vidt angår biologiske og kemiske våben, forskning og udvikling

g) spredning af farlige stoffer, brandstiftelse, fremkaldelse af oversvømmelser eller eksplosioner med den følgevirkning, at menneskeliv bringes i fare

lemsstater automatisk skal deles med Europol (Peissl, 2003, s. 20). Eksempelvis er det i Frankrig besluttet, at serviceudbydere skal gemme bestemte data i op til 12 måneder, ligesom det er gjort nemmere for politiet at få ransagningskendelser til at undersøge private huse og biler (Peissl, 2003, s. 20).

I Storbritannien har en antiterrorpakke, der blev indført efter 11/9 2001, haft den betydning, at bestemte grupper af mistænkte nu kan tilbageholdes på ubestemt tid uden retssag (Peissl, 2003, s. 19-20). Denne ændring indebærer helt konkret, at Storbritannien nu fraviger art. 5, stk. 1[12] i "Europarådets Konvention til Beskyttelse af Menneskerettigheder og Grundlæggende Frihedsrettigheder" (herefter blot Menneskerettighedskonventionen), der omhandler frihed og personlig sikkerhed (Dyer, 2002; Folketingets EU-oplysning; Peissl, 2003, s. 19).

I 2013 blev det i offentligheden kendt, at det britiske Government Communications Headquarters (herefter blot GCHQ) har forbindelser til det amerikanske NSA. GCHQ har eksempelvis tappet data fra fiberoptiske kabler for derefter at gemme disse data i 30 dage, hvor de så kan blive undersøgt. Disse data er blevet delt med NSA – data om både uskyldige mennesker og om mistænkte. En kilde har til The Guardian udtalt, at kriterierne for, om data er interessante for GCHQ: "[...] are security, terror, organised crime." (MacAskill, Borger, Nick, Davies, & Ball, 2013). Således er offentlig sikkerhed igen en begrundelse for at indsamle data.

---

h) forstyrrelseeller afbrydelse af vand- eller elforsyningen eller forsyningen med andre grundlæggende naturressourcer med den følgevirkning, at menneskeliv bringes i fare

i) fremsættelse af trusler om at ville begå en af de i litra a) til h) nævnte handlinger." (EU-Oplysningen).

[12] I art. 5, stk. 1 står der blandt andet, at:"[...] Enhver har ret til frihed og personlig sikkerhed. Ingen må berøves friheden undtagen i følgende tilfælde og i overensstemmelse med den ved lov foreskrevne fremgangsmåde: a) lovlig forvaring af en person efter domfældelse af en kompetent domstol; [...]". (Folketingets EU-oplysning, uddrag fra art. 5).

I Danmark blev den såkaldte antiterrorpakke I[13] hastigt vedtaget og implementeret i kølvandet på hændelserne den 11/9 2001. Terrorpakken omfattede en række ændringer i straffeloven, retsplejeloven, våbenloven og udleveringsloven (Justitsministeriet). Blandt andet vedtog man den 2. juni 2002: "[...] en pligt for teleselskaber og internetudbydere til at registrere og i 1 år opbevare de oplysninger, der er relevante for politiets indgreb i meddelelseshemmeligheden." (Justitsministeriet), hvilket skulle tjene til at forbedre af politiets muligheder i forbindelse med opklaringsarbejde (Institut for Menneskerettigheder, 2013, s. 12).

Som en reaktion på terrorangrebet i London i 2005 kom endnu en terrorpakke i Danmark: Terrorpakke II[14]. Med Terrorpakke II fulgte den ofte omtalte Logningsbekendtgørelse, der indeholdt ændringer og udvidelser i mulighederne for at overvåge telekommunikation og anden kommunikation såsom e-mails, sms- og mms-beskeder og surfing på internettet (Lovbekendtgørelse nr. 988 af 28. september 2006).

Logningsbekendtgørelsen var en implementering af Logningsdirektivet, 2006/24/EF[15] (Europa-parlamentets og rådets direktiv, 2006). Af Logningsdirektivet fremgår det, at det er valgfrit for medlemsstaterne, hvor længe de vil pålægge serviceudbyderne at opbevare de indsamlede data – dog som minimum i 6 måneder og maksimalt i 24 måneder. I Danmark besluttede man, at data skulle gemmes i den længst mulige periode, altså 24 måneder. Baggrunden for udvidelsen af logningsforpligtigelsen i Danmark i forhold til Logningsdirektivets minimumskrav var ifølge Justitsministeriet, at Danmark allerede tilbage i 2006 havde udbredt brug af højhastighedsinternet.

[13] Det fulde navn er: "Lov om ændring af straffeloven, retsplejeloven, lov om konkurrence- og forbrugerforhold på telemarkedet, våbenloven, udleveringsloven samt lov om udlevering af lovovertrædere til Finland, Island, Norge og Sverige.".

[14] Det fulde navn er: "Lov om ændring af straffeloven, retsplejeloven og forskellige andre love.".

[15] Det fulde navn er :"EUROPA-PARLAMENTETS OG RÅDETS DIREKTIV 2006/24/EF af 15. marts 2006 om lagring af data genereret eller behandlet i forbindelse med tilvejebringelse af offentligt tilgængelige elektroniske kommunikationstjenester eller elektroniske kommunikationsnet og om ændring af direktiv 2002/58/EF."

Der har været megen kritik af Logningsdirektivet og også af den danske implementering heraf. Beskyldninger har blandt andet lydt på, at foranstaltningerne var særdeles problematiske og kompromitterende for individets privathed. Det tog også omkring fem år at implementere Logningsbekendtgørelsen[16] grundet blandt andet utilfredshed fra teleselskabernes side (Institut for Menneskerettigheder, 2013, s. 12). Institut for Menneskerettigheder og Datatilsynet: "[...] påpegede i den forbindelse, at det ikke syntes sandsynliggjort, at logningspligten var et nødvendigt og proportionalt tiltag i et demokratisk samfund." (Institut for Menneskerettigheder, 2013, s. 12).

Det var særdeles omfattende mængder data, der blev indsamlet i Danmark. I 2010 anslog man, at der blev foretaget omkring 100.000 registreringer pr. borger pr. år, og i 2012 blev der foretaget cirka 144.000 registreringer pr. borger pr. år. På landsplan svarer det til 900 milliarder registreringer i 2012 (Institut for Menneskerettigheder, 2015, s. 15-16). Det har vist sig, at Logningsbekendtgørelsen primært er blevet anvendt i forhold til kriminalitet, der ikke har været terrorrelateret. Dette forhold er interessant, når netop terror var begrundelsen for at logge data (Institut for Menneskerettigheder, 2015, s. 15). Den særlige danske sessionslogning har ligeledes har kun været efterspurgt af politiet i yderst begrænset omfang (Institut for Menneskerettigheder, 2015, s. 16).

Den 8. april 2014 traf EU-domstolen afgørelse om, at Logningsdirektivet var ugyldigt. Det var domstolens opfattelse, at direktivet ikke var i overensstemmelse med art. 7 om respekt for privatliv og familieliv, art. 8 om beskyttelse af personoplysninger og art. 52 (1) om rækkevidde og fortolkning af rettigheder og principper i Den Europæiske Unions Charter om Grundlæggende Rettigheder (Judgement of the court (Grand Chamber), 2014, s. paragraf 69). Således vurderede domstolen, at direktivet krænkede privatlivets fred.

EU-domstolens dom gav anledning til, at justitsministeriet måtte vurdere, om Logningsdirektivets ugyldighed havde betydning for den danske Logningsbekendtgørelse, idet denne var baseret på Logningsdirektivet. Justitsministeriet

[16] Bekendtgørelsen trådte i kraft den 15. september 2007.

konkluderede, at Logningsbekendtgørelsen ikke er i strid med Den Europæiske Unions Charter om Grundlæggende Rettigheder. Der blev lagt vægt på, at Logningsbekendtgørelsen indeholder en række bestemmelser, der adskiller sig fra Logningsdirektivet – disse er efter justitsministeriets udsagn "[...] klare og præcise [...]" (Justitsministeriet, 2. juni, 2014, s. 30), hvorfor risiko for ulovlig adgang til og brug af data er sikret i væsentlig grad (Justitsministeriet, 2. juni, 2014, s. 21).

I forlængelse heraf ændrede man dog alligevel Logningsbekendtgørelsen således, at der ikke er adgang til at udføre sessionslogning – det vil sige logning af internettrafik (Lovbekendtgørelse nr. 660 af 19. juni 2014). Det bemærkes, at Logningsbekendtgørelsens bestemmelser om sessionslogning ikke udspringer af Logningsdirektivet (Institut for Menneskerettigheder, 2015, s. 16). Ændringen gennemføres, idet det viser sig, at disse data ikke er brugbare til det formål, de var tiltænkt (Justitsministeriet, 2. juni, 2014, s. 21). Justitsministeriet gør netop dette forhold klart, idet man bemærker, at der kun "[...] i meget begrænset omfang [...]" (Justitsministeriet, 2. juni, 2014, s. 21) har været brug for oplysninger fra sessionslogning i forbindelse med efterforskning og retsforfølgning af strafbare forhold.

Justitsministeriet mener dog, at den manglende anvendelighed af de indsamlede data kan skyldes, at teleselskaberne er i deres gode ret til kun at indsamle én ud af hver 500 datapakker, som en bruger genererer ved sin kommunikation på nettet. Om justitsministeriet mener, at såfremt man indsamlede flere data, så ville funktionen af indsamling blive den ønskede, er ikke eksplicit berørt i notatet (Justitsministeriet, 2. juni, 2014, s. 21).

Justitsministeriets opfattelse bliver nu formentlig indirekte prøvet i forbindelse med en svensk retssag. Et svensk teleselskab har anlagt sag mod den relevante svenske myndighed, Post- og telestyrelsen, da det er det svenske teleselskabs opfattelse, at det som konsekvens af Logningsdirektivets ugyldighed har adgang til at slette al data lagret i medfør af den svenske implementering af dette direktiv (Justitsministeriet, 2015).

Da retssagen involverer fortolkning af EU-lovgivning, har den svenske domsyol forelagt EU-domstolen et præjudicielt spørgsmål om, hvorvidt den svenske lovgivning, der forpligter teleudbydere til at lagre trafikdata, er forenelig med EU-retten, herunder Den Europæiske Unions Charter om grundlæggende rettigheder (Justitsministeriet, 2015).

Den svenske lovgivning på området (den svenske implementering af Logningsdirektivet) har væsentlige fællestræk med den danske Logningsbekendtgørelse, og Justitsministeriet har derfor i sommeren 2015 afgivet et indlæg vedrørende den danske regerings opfattelse af retsstillingen på området (Justitsministeriet, 2015).

I Danmark har den tidligere socialdemokratiske regering efter terrorangrebene i Paris januar 2015 og i København februar 2015 fremlagt et forslag om 12 tiltag mod terror (Regeringen, 2015, s. 5). Prisen herfor er 970 millioner kr. over fire år. Pengene skal blandt andet gå til udvidelse af overvågningskapaciteten imod enkeltpersoner og trusler mere generelt samt til et nyt it-system med henblik på bedre at kunne udnytte viden fra de data, der er tilgængelige. Man planlægger også at ansætte personale: "[...] til strategisk, operativ og taktisk analyse og bearbejdning af data. Det vil give nye muligheder for at arbejde mere proaktivt, effektivt og integreret med efterforskning, monitering, analyse og afværgelse af terrorangreb." (Regeringen, 2015, s. 5). Lovforslaget er endnu ikke vedtaget, men ideen er eksplicit, at indsamling og behandling af data skal styrke sikkerheden.

1.2. SIKKERHEDSTRUSLER MOD DEN EUROPÆISKE UNION

Det er i ovenstående afsnit anskueliggjort, at EU, USA og en række EU-lande gør en væsentlig indsats for at sikre den offentlige sikkerhed. I EU's seneste sikkerhedsstrategi fra 2003 blev det slået fast, at EU i dag er mere sikker end nogensinde før (Den Europæiske Union, 2003, s. 1). De trusler, man til trods herfor oplever, har ændret sig væsentlig over tid. EU's sikkerhedsstrategi sigter i dag mod fem bredt definerede nøgletrusler: Terror, spredning og anvendelse af masseødelæggelsesvåben, regionale konflikter, statssammenbrud og organiseret kriminalitet (Den Europæiske Union, 2003).

I afhandlingen vil der blive fokuseret på to af de fem sikkerhedstrusler, nemlig terror og organiseret kriminalitet. Disse er netop de former for kriminalitet, som sikkerhedsteknologierne, der er relevante for afhandlingens problemstilling vedrørende indsamling af data, behandler.

Om terror står der i EU's sikkerhedsstrategi, at det:

> "[...] puts lives at risk; it imposes large costs; it seeks to undermine the openness and tolerance of our societies, and it poses a growing strategic threat to the whole of Europe. Increasingly, terrorist movements are well-resourced, connected by electronic networks, and are willing to use unlimited violence to cause massive casualties.". (Den Europæiske Union, 2003, s. 3).

Organiseret kriminalitet er beskrevet således:

> "Europe is a prime target for organised crime. This internal threat to our security has an important external dimension: cross-border trafficking in drugs, women, illegal migrants and weapons accounts for a large part of the activities of criminal gangs. It can have links with terrorism." (Den Europæiske Union, 2003, s. 4).

Sikkerhedstruslerne mod EU har blandt andet ændret sig som følge af den udbredte anvendelse af teknologi og internettets komme. Europol gør også dette klart i sin rapport fra 2014, "The Internet Organised Crime Threat Assessment 2014" (også kaldet iOCTA-14) (EUROPOL, 2014), hvor det konstateres, at internettet, i kraft af at man ikke behøver at være fysisk tilstede for at udføre noget kriminelt, netop understøtter muligheder for kriminalitet (EUROPOL, 2014, s. 5, 9). I dag er truslerne mod EU langt mere dynamiske end tidligere, og af samme grund er det nødvendigt, at der føres en mere aktiv sikkerhedspolitik fra EU's side. Formålet med den aktive sikkerhedspolitik er grundlæggende at forebygge, og det ekspliciteres i sikkerhedsstrategien, at man ønsker at være klar til handling, før en trussel opstår, ligesom at forebyggelse af konflikter og trusler generelt ikke kan iværksættes for tidligt (Den Europæiske Union, 2003, s. 7). Forebyggelse kan omfatte blandt andet overvågning og såkaldt proaktiv *dataveillance*. Det betyder samtidigt, at man vil forsøge at indsamle så mange data som muligt for at kunne forudsige, hvad der vil ske (Raguse, Meints, Langfeldt, & Peissl, 2008, s. 22).

1.3. *DATAVEILLANCE* SOM OVERVÅGNINGSFORM

Denne afhandling er afgrænset således, at de sikkerhedsteknologier, der behandles, anvendes til at overvåge data. Dataovervågning benævnes ofte dataveillance (Clarke, 1988). I afhandlingen vil kun digitaliserede data blive taget i betragtning, til trods for at *dataveillance* principielt også kan foretages ved anvendelse af ikke-digitaliserede data. Overvågning af digitale data findes særligt interessant, idet teknologien, der anvendes til overvågning, til stadighed bliver mere avanceret og hastigt udvikles. Desuden vokser mængden af data kraftigt, hvorfor grundlaget for at foretage overvågning heraf stedse forbedres.

Det er vigtigt at slå fast, at overvågning og såkaldt *dataveillance* i denne afhandling ikke opfattes som aktiviteter, der nødvendigvis er et onde eller nødvendigvis er et gode i en demokratisk stat. Overvågning tillægges som udgangspunkt ikke nogen værdi. Man kan argumentere for, at disse midler *bør* anvendes i nogle sammenhænge, idet fordelene herved *kan* være signifikante (Clarke, 1988, s. 505-506).

Termen *dataveillance* blev nævnt for første gang af Roger Clarke i 1988 i den klassiske artikel "Information Technology and Dataveillance" og defineres her som: *"*[...] the systematic use of personal data systems in the investigation or monitoring of the actions or communications of one or more persons*."* (Clarke, 1988, s. 499). *Dataveillance* adskiller sig fra mere traditionel overvågning ved, at man ikke overvåger en person, men data *om personen,* og *dataveillance* udpeger således en bestemt måde at overvåge på*.* Med andre ord er der tale om en slags data-skygge af den overvågede person, et *digitalt individ*[17]. Der kan også være tale om overvågning af en gruppe personer, som det vil gøre sig gældende i forbindelse med masseovervågning (Clarke, 1993a).

Man kan med overveje, om det er meningsfuldt at anvende termen *dataveillance* nu til dags, idet it er blevet allestedsnærværende, og dermed er muligheden for overvågning også allestedsnærværende (Lauritsen, 2011, s. 55).

[17] Egen oversættelse af "digital individual" (Clarke, 1993a).

Idet man med termen udpeger systematisk overvågning af *personal data systems,* mener jeg dog stadig, at der er grund til at bibeholde *dataveillance* som begreb i afhandlingen. Samtidigt betoner Clarke det forhold, at der er tale om *overvågning af data* eller *information* (Clarke, 1988, s. 499). Peter Lauritsen bemærker også, at begrebet: "[...] peger på de enorme registreringsmuligheder, som netop it rummer" (Lauritsen, 2011, s. 55). Muligheden for registrering af individer i databaser er et centralt aspekt i den problemstilling, som jeg behandler – det kan således siges at være en betingelse for problemstillingen.

Digitaliserede data, som her behandles, er af James Moor karakteriseret som såkaldt *greased data*[18]. *Greased data* er kendetegnet ved at være svære at holde fast i, nemt flytbare, søgbare og findbare, ligesom de kan tilgås igen og igen (Moor J. H., 1997, s. 27). De store mængder *greased data*, som vi har at gøre med i dag, udgør tilsammen et solidt fundament for udøvelse af *dataveillance*. Ydermere øges mulighederne for at udføre *dataveillance*, idet en lang række aktiviteter i dag har ændret karakter og er blevet *informationsberigede*[19], hvilket såvel Moor som Helen Nissenbaum påpeger (Moor J. , 1998, s. 15; Nissenbaum, 2010, s. 23-24).

Almindelige dagligdags gøremål, der tidligere kun inkluderede brug af fysiske objekter, er nu i højere grad blevet et spørgsmål om *overførsel af information*. To eksempler herpå, hvor der endvidere også gøres brug af såkaldte lokationsbaserede[20] data, er anvendelse af betalingskort og mobiltelefoni: I dag er det ofte nemmere at betale sine varer med et betalingskort end kontant. En simpel betaling for kaffe på en cafe bliver således en aktivitet, der muliggør indsamling af information om, hvor en person har været på et givent tidspunkt (Nissenbaum, 2010, s. 24). Mobiltelefoner er ligeledes blevet langt mere

[18] Begrebet er ikke oversat, da der ikke findes en passende dansk betegnelse (Moor J. H., 1997, s. 27).

[19] Egen oversættelse af "informationally enriched" (Moor J. , 1998, s. 15).

[20] Lokationsbaseret teknologi er her defineret som "[...] technological means that allow the identification og a location of a location. A location can be defined as a position relative to the surface of the earth." (van Loenen, Groetelaers, Zevenbergen, & de Jong, 2007, s. 135).

avancerede end tidligere. Dette forhold medfører, at brugen af mobiltelefon kan give et særdeles præcist billede af en persons sociale netværk, når det undersøges, hvem personen har været i kontakt med ved opkald og sms. Da mobiltelefoni er en lokationsbaseret teknologi, er det muligt at udpege, hvor en person har befundet sig og på hvilke tidspunkter. Det bliver således svært at forsvinde eller gemme sig (van Loenen, Groetelaers, Zevenbergen, & de Jong, 2007, s. 136). Omvendt skal det bemærkes, at selvom teknologien giver mulighed for, at man kan indsamle lokationsbaserede data, så følger det ikke *per se*, at nogen skal indsamle disse data.

Nissenbaum påpeger i forbindelse med ovenstående, at for teknologi, der genererer data, som efterfølgende kan overvåges, var brug til dataindsamling og overvågning ofte ikke intenderet i udgangspunktet. Dette gør sig også gældende for mange af de data, man i dag analyserer (Nissenbaum, 2010, s. 24). Det var trods alt ikke intentionen med betalingskortet, at man ville have muligheden for at følge med i, hvor en person har været. Man kan derfor tale om en *sekundær overvågningskapacitet* [21].

Dataveillance er af en række grunde en særdeles attraktiv overvågningsform. For det første er den billig, da den er væsentligt mindre arbejdskrævende end traditionel overvågning (Clarke, 1988, s. 501). For det andet er overvågning af data relativt let at igangsætte, idet der ofte kun kræves mindre ændringer i allerede eksisterende systemer, hvilket er i modsætning til eksempelvis kameraovervågning, der kræver et betydeligt arbejde at iværksætte og formentlig også en betydelig ingeniørmæssig indsigt. For det tredje er *dataveillance* fleksibel, idet udbredelsen af internettet og World Wide Web gør det muligt at indsamle, flytte og lagre data, hvor end vi ønsker (Nissenbaum, 2010, s. 40). For det fjerde kan indsamling og anvendelse af data foregå asynkront, og data kan genbruges igen og igen til forskellige formål, der ikke i udgangspunktet forekommer åbenlyse eller planlagte. Brugen af d*ataveillance* betyder også, at langt flere mennesker på én gang kan overvåges, idet denne form for overvågning kan automatiseres og er: "[...] essentially computerbased, with the "watch

[21] Egen oversættelse af "Secondary surveillance capacity" (Nissenbaum, 2010, s. 24).

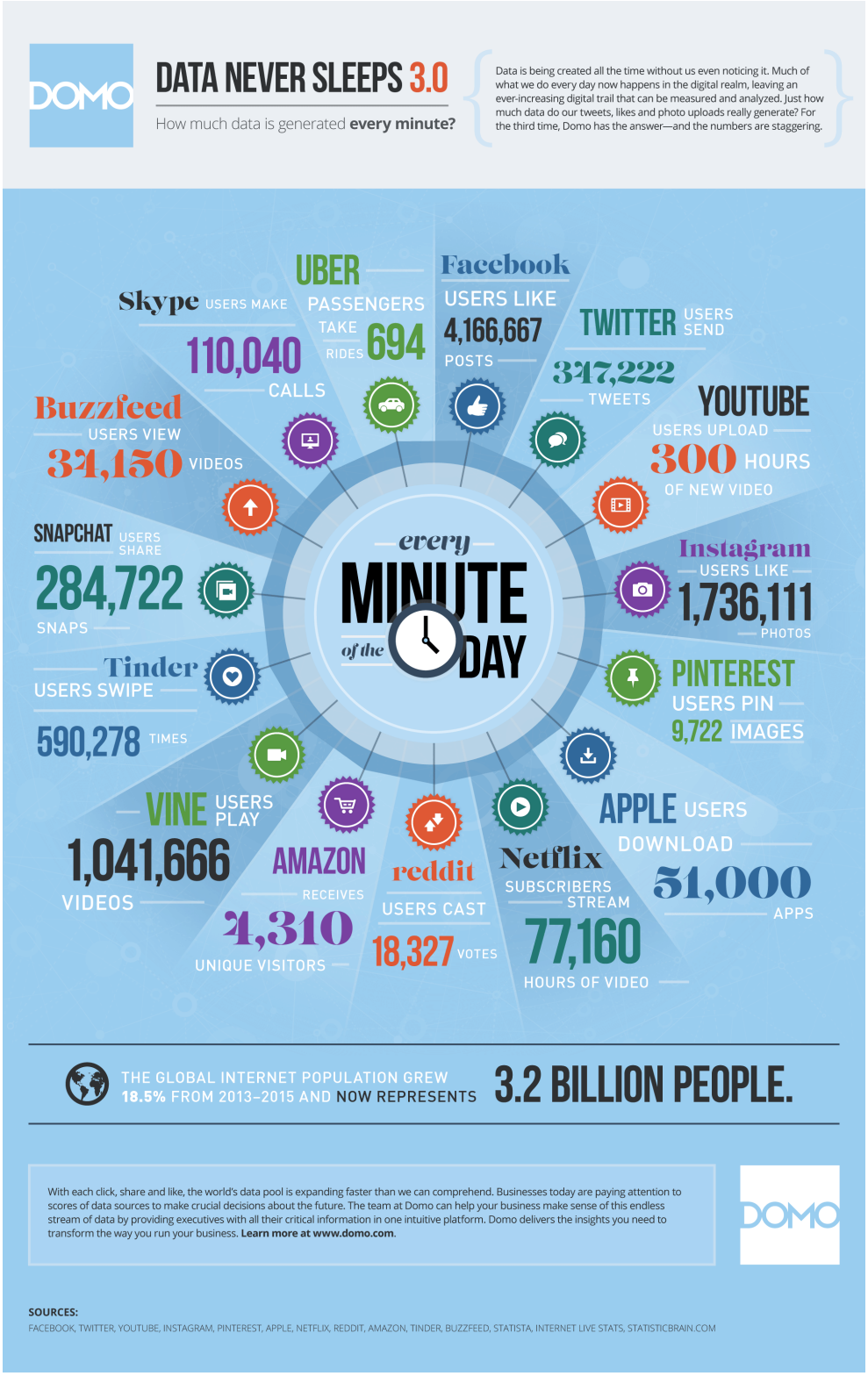
and report" responsibility delegated to a reliable, ever-wakeful servant." (Clarke, 1988, s. 501).

Idet nærværende afhandling grundlæggende er et teoretisk, it-etisk projekt, er det relevant at anskue såvel tekniske som humanistiske og sociale aspekter i samspil. Dette er vigtigt for forståelsen af, at *dataveillance* påvirkes af både tekniske og menneskelige forhold og på samme tid kan siges at være et produkt af begge (Lyon, 2007, s. 21). Man kan endvidere argumentere for, at netop teknologien har været med til at ændre overvågningens fundament og mulighederne herfor drastisk. Samtidigt med at *dataveillance* kan anvendes til at øge den offentlige sikkerhed, så medfører *dataveillance* også en risiko for, at individers privathed krænkes ligesom en række andre mere basale rettigheder som eksempelvis frihed og autonomi kompromitteres. Disse forhold er samlet set med til at aktualisere nærværende afhandling.

1.3.1. *DATAVEILLANCE* AF *BIG DATA* SOM SIKKERHEDSTEKNOLOGI

Dataveillance skal ifølge David Lyon ikke ses som resultatet af terror eller 11/9 2001 alene. Disse har blot været medvirkende incitamenter til overvågning, globalisering og digitalisering. Det er heller ikke udelukkende et spørgsmål om styrkelse af bureaukratiske kræfter. Det er derimod en kompleks proces: "[...] in which digital technologies and personal data are fundamentally implicated and meet in the software coding nexus." (Lyon, 2007, s. 115).

Data, en kritisk ressource for *dataveillance*, eksisterer i dag i overflod. Billede 1 er en grafisk repræsentation og katalogisering, der demonstrerer, hvor mange data der på verdensplan genereres hvert eneste minut:



Billede 1: Info-grafik (https://web-assets.domo.com/blog/wp-content/uploads/2015/08/15_domo_data-never-sleeps-3_final1.png)

I dag taler man ikke blot om data, men om såkaldt *big data*[22]. *Big data* lider dog under at være vagt defineret (Floridi, 2012, s. 436). Umiddelbart leder betegnelsen *big data* tankerne hen på kvantitative forhold – der må være tale om store mængder data. Den tidligere canadiske Information & Privacy Commissioner Ann Cavoukians definition af *big data* er et eksempel på netop dette forhold, idet hun skriver, at *big data* er: "[...] datasets whose size is beyond the ability of typical database software tools to capture, store, manage, and analyze." (Cavoukian, 2012c, s. 7). Denne type af definition støder man jævnligt på, når *big data* forsøges defineret (McKinsey Global Institute, 2011, s. 1; Wikipedia, big data). *Big data* opfattes ikke i afhandlingen som noget, der primært handler om volumen i absolut forstand eller om en bestemt mængde af computerkraft. *Big data* udpeger derimod de forudsigelser, som vi kan generere ved at anvende *big data.*

Omkring 70 procent af al *big data* er brugergenereret, og et typisk eksempel på *big data* er data fra sociale medier. Den øvrige del stammer fra offentligt tilgængelige data, forskning og finansielle transaktioner for blot at komme med nogle få eksempler (Craig & Ludloff, 2011, s. 4). *Big data* er spået en stor fremtid, idet disse data siges at have indflydelse på verdensøkonomien, samfundet og endda videnskaben (Mayer-Schönberger & Cukier, 2013, s. 11; McKinsey Global Institute, 2011; European Commission, 2014c; Floridi, 2012, s. 436).

I EU forventer man, at teknologi og services, der hviler på *big data,* vil stige til en værdi af 16.9 milliarder US dollars i 2015. I Storbritannien alene forudser man, at antallet af *big data*-specialister i større firmaer vil vokse med 240 % over de kommende år (European Commission, 2014c, s. 2). Potentialet for at anvende *big data* som grundlag for *dataveillance* er ligeledes stort og menes at kunne give signifikante samfundsrelaterede fordele (Mayer-Schönberger & Cukier, 2013, s. 7).

Ifølge Hilbert befinder vi os midt i et paradigmeskift fra informationssamfund til videnssamfund (Hilbert, 2013, s. 4). Dette viser sig derved, at *big data* giver

[22] *Big data* anvendes også i dansk sprogbrug, hvorfor termen ikke er oversat.

forbedrede forudsætninger for at forudsige fremtiden. Den grundlæggende antagelse om sådanne forudsigelser er, at såfremt man kan blive bevidst om afvigelser, før de forekommer, eller netop idet de forekommer, vil dette give et langt bedre fundament for at kunne reagere og dette endda proaktivt, hvilket også gælder i forhold til politiets arbejde (Mayer-Schönberger & Cukier, 2013, s. 59; Perry, McInnis, Price, Smith, & Hollywood, 2013, s. 1-2).

Tidligere, når vi traf beslutninger på baggrund af dataanalyse, var disse principielt reaktive handlinger (Bacher, 2013, s. 9). De "forudsigelser", vi her foretog (også i forbindelse med politiarbejde), byggede nødvendigvis på grundlæggende ideer eller forhåbninger om, at fremtiden artede sig som fortiden. Dette har været brugbart, såfremt vores spådom var rigtig. Var dette ikke tilfældet, var man i virkeligheden lige vidt med sådanne reaktive analyser og handlinger. Det er derfor en væsentlig ændring, at analyse, der hviler på *big data,* nu i betydelig grad kan kvalificere forudsigelser og dermed finde anvendelse med henblik på specifikt at opretholde den offentlige sikkerhed til gavn for stat såvel som for individ. Et eksempel herpå er *predictive policing.*

I nærværende afhandling er *big data* behandlet som en ressource for *dataveillance*, hvis formål er at opretholde offentlig sikkerhed. Dataveillance kan danne grundlag for *kriminalitetsanalyse,* der er et paraplybegreb, hvormed politiet udpeger: "[...] patterns and relationships between crime data and other relevant data sources to prioritize and target police activity." (Cope, 2004, s. 188).

Med anvendelse af *big data* kan *dataveillance* således fungere som en sikkerhedsteknologi, hvor den grundlæggende ide går hånd i hånd med EU's erklærede hensigt om at være mere aktiv i forsøget på at opnå strategiske mål (Den Europæiske Union, 2003, s. 11). Dette kan blandt andet tilskrives det forhold, at man i dag kan analysere *big data* med en sådan hastighed, at det er muligt at reagere på faktiske forhold i realtid. Det mest interessante ved *big data* er med andre ord ikke kvantiteten af data alene, men også de muligheder *big data* understøtter for analyse og efterfølgende som grundlag for *intelligent*

beslutningstagning [23] (Bacher, 2013, s. 32; Hilbert, 2013, s. 4-5; Mayer-Schönberger & Cukier, 2013, s. 6).

Anvendes data som grundlag for intelligente beslutninger med henblik på at fremme offentlig sikkerhed, kan der være tale om *intelligence-led policing*[24] (herefter blot ILP), der i afhandlingen bliver opfattet som en ledelsesfilosofi (Ratcliffe, 2011, s. 89). ILP som ledelsesfilosofi kan give anledning til anvendelse af en række metoder. Der gives eksempler herpå i nærværende afhandlings kapitel 7, *Dataveillance* af *big data* som sikkerhedsteknologi. En af disse metoder er såkaldt *predictive policing*[25] (Bacher, 2013, s. 7).

Politi rundt om i verden forsøger at forudsige kriminalitet ved hjælp af *predicitve policing*, hvilket blandt andet kan bestå i, at man anvender offentligt tilgængelig *big data*, der er høstet fra sociale medier. Ideen her er, at det er muligt at foretage probabilistiske analyser på baggrund af eksisterende data for på den måde at kunne forudsige, hvad der *sandsynligvis* kommer til at ske (Bacher, 2013, s. 14). Disse data kan i realtid sammenkøres med historiske kriminalitetsrelaterede data fra politiets egne databaser. På baggrund heraf kan man statistisk forudsige sandsynligheden for kriminalitet. Med disse forudsigelser bliver det muligt at forbedre ressourceallokering og foretage mere kvalificeret og intelligent beslutningstagning politiets arbejde (Bacher, 2013, s. 18; Mayer-Schönberger & Cukier, 2013, s. 11; Perry, McInnis, Price, Smith, & Hollywood, 2013, s. xxii, 127).

Et konkret eksempel på en sikkerhedsteknologi, hvormed man forsøger at forudsige kriminalitet, stammer fra forskere ved University of Virginia, der har udviklet og testet et system, der netop i realtid kan kortlægge geo-taggede

[23] Egen oversættelse af "Intelligent decision-making" (Hilbert, s. 4).

[24] Begrebet kan oversættes til "efterretninger". Jeg har dog valgt at fastholde det engelske begreb.

[25] Begrebet er ikke oversat, da der ikke findes en passende dansk betegnelse.

tweets[26] fra det sociale medie Twitter med henblik på at forudsige kriminalitet lokalt på baggrund af geografiske forhold[27]. Ønsket er særdeles præcist at kunne forudsige, hvor kriminalitet vil forekomme og det gerne helt ned på husblokniveau. I og med at *tweets* ofte er offentligt tilgængelige, er Twitter med sin 140 millioner brugere på verdensplan og 380 millioner *tweets* pr. dag et særligt brugbart medie til denne form for forudsigelser[28] (Gerber, 2014, s. 115).

Modellen i det omtalte system udfører en lingvistisk analyse af *tweets* fra Twitter. I analysen leder modellen efter en korrelation mellem frekvensen af aktiviteter og frekvensen af kriminalitet i specifikke områder. Data, der høstet fra Twitter og siden analyseret, kombineres dernæst med historiske data om kriminalitet fra det samme område[29]. Hvis personer *tweeter* om at gå i byen, drikke alkohol eller tage til sportsbegivenheder, hvilket alle er eksempler på aktiviteter, der korrelerer med kriminalitet, så kan man deraf udlede, at det er sandsynligt, at der vil forekomme kriminalitet i et bestemt område (Pearson, 2014). Idet disse *tweets* netop er geo-taggede, kan disse indikatorer på kriminalitet afgrænses geografisk, og dermed kan *hot spots* udpeges i realtid.[30]

---

[26] Et *tweet* er en maksimalt 140 tegn lang tekststreng. Hvorvidt man ønsker at lade sit *tweet* indeholde en attribut med information om ens geografiske position (geo-tag), er op til den enkelte bruger.

[27] Der tages ikke højde for temporale forhold i denne analyse. Såfremt databehandlingen behandlede de temporale data, som er indeholdt i et *tweet*, ville man formentlig kunne udføre en mere præcis databehandling (Gerber, 2014, s. 122).

[28] Hermed er det dog ikke sagt, at der ikke kan være visse metodologiske problemer forbundet med at anvende Twitter som datakilde. Denne diskussion tages op i kapitel 7., *Dataveillance af big data som sikkerhedsteknologi,* om *big data* som ressource for ILP.

[29] De indsamlede data i studiet bestod konkret af data om alle dokumenterede forbrydelser fra 1. januar 2013 til 31. marts 2013 i Chicago – i alt 60.876 forbrydelser. Data om hver forbrydelse indeholdt blandt andet information om tidspunkt for forbrydelsen, data om længdegrad og breddegrad på husblok-niveau og kriminalitetstype. De indsamlede Twitter-data fra samme periode indeholdt GPS-data, der gjorde det muligt kun at indsamle data fra Chicago. I alt blev der indsamlet 1,528,184 *tweets* (Gerber, 2014, 116).

[30] Det *hot spot map,* der omtales i dette eksempel, er udformet på baggrund af en såkaldt "kernel density estimation" (KDE), der er en statistisk metode. Det ligger dog uden for afhandlingens område at behandle KDE nærmere (Gerber, 2014).

I studiet fandt man, at der i 19 af 25 forskellige typer af kriminalitet var en forbedring i forudsigelsen af kriminalitet ved anvendelse af *tweets* i analysearbejdet sammenholdt med traditionel *hot spot mapping*, hvor man ikke anvender realtidsdata, men blot forskellige historiske data (Gerber, 2014, s. 116, 121). Traditionel *hot spot mapping* er en reaktiv metode, hvormed man analyserer og visualiserer fordeling af kriminalitet i forhold til tidsmæssige og geografiske faktorer.

Som det er demonstreret med eksemplet ovenfor, så kan brugen af *big data* medføre en række fordele med hensyn til opretholdelse af offentlig sikkerhed. Samtidigt er dette dog også ensbetydende med øget overvågning, hvilket *kan* lede til en krænkelse af individets privathed. Spændingen mellem privathed og offentlig sikkerhed er med andre ord til stede i sikkerhedsteknologi.

Man kan argumentere for, at det er væsentligt at reflektere over værdier i forbindelse med, at en given teknologi udvikles. Et sådant syn på (sikkerheds-)teknologi og udvikling heraf er i overensstemmelse med såvel VSD som PbD, der begge er pragmatiske tilgange til proaktivt at realisere værdier i teknologi. Igen må det nævnes, at VSD og PbD hviler på et interaktionsperspektiv på teknologi, hvorved teknologideterminisme afvises. At realisere bestemte værdier i teknologi implicerer således ikke nødvendigvis en bestemt anvendelse – der er tale om, at teknologien kan understøtte eller vanskeliggøre en bestemt anvendelse til en vis grad. Tilgangene vil med udgangspunkt i en pragmatisk forståelse blive inddraget med henblik på at diskutere deres anvendelighed i forhold til sikkerhedsteknologi.

1.4. IMPLIKATIONER AF OVERVÅGNING OG *DATAVEILLANCE*

Clarke fastslår om *dataveillance*, at: "[...] dataveillance is, by its very nature, intrusive and threatening." (Clarke, 1988, s. 506). *Dataveillance* har således potentialet til at skabe en række af problemstillinger for individer eller grupper af individer. Clarkes karakteristik af *dataveillance* som nærgående og truende synes især at gælde, når overvågningen foretages af *de mange*[31], hvilket

[31] Clarke refererer i artiklen "Information Technology and Dataveillance" (Clarke, 1988) til dette som "mass surveillance".

står i kontrast til *dataveillance af individet*[32]. *Dataveillance* af individet sker, hvis et individ af den ene eller anden grund har tiltrukket sig opmærksomhed. *Dataveillance* af individet sker ofte for at diskvalificere et individ i forhold til eksempelvis ansøgte offentlige ydelser, et job eller lignende. Under andre omstændigheder udfører man overvågning, fordi en person har foretaget noget usædvanligt, eller man har en mistanke herom. Ved *masseovervågningen*[33] overvåger man ikke en bestemt person, men derimod en gruppe. *Masseovervågningen* foregår uden forudgående mistanke som en rutinehandling, på baggrund af hvilken en mistanke så efterfølgende kan rejses. Denne form for overvågning udføres eksempelvis af NSA ved hjælp af XKeyscore (Greenwald, 31. juli, 2013).

Masseovervågning som praksis kan lede til en kultur, hvor alle mistænkeliggør alle (Ball, Lyon, Wood, Norris, & Raab, 2006, s. 3; Clarke, 1988, s. 503, 508). Masseovervågning kan helt konkret komme til udtryk som såkaldt profilering, der er en teknik, hvormed en bestemt klasse af personer er: "[...] inferred from past experience, and data holdings are then searched for individuals with a close fit to that set of characteristics." (Clarke, 1993b, s. 405). Profilering kan have den utilsigtede konsekvens, at man kan ende i en "kasse", som man egentlig ikke tilhører.

Kendetegnende for nogle former for overvågning er det asymmetriske forhold mellem den, der bliver overvåget, og den, der overvåger. Walter Peissl forstår overvågning som en sekvens af kontrol-handlinger (Peissl, 2003, s. 21), og i lighed hermed beskriver Lyon den asymmetriske relation, hvor den overvågende er den privilegerede part, som et grundlæggende særkende ved overvågning (Lyon, 2007, s. 15). Denne asymmetriske magtrelation er ligeledes omdrejningspunktet for den britiske tænker og utilitarist Jeremy Benthams (1748-1832) berømte ide fra 1791 om fængslet eller inspektionshuset[34], Panoptikon (Bentham, 1843, s. 39). Panoptikon byggede på opsynsprincippet,

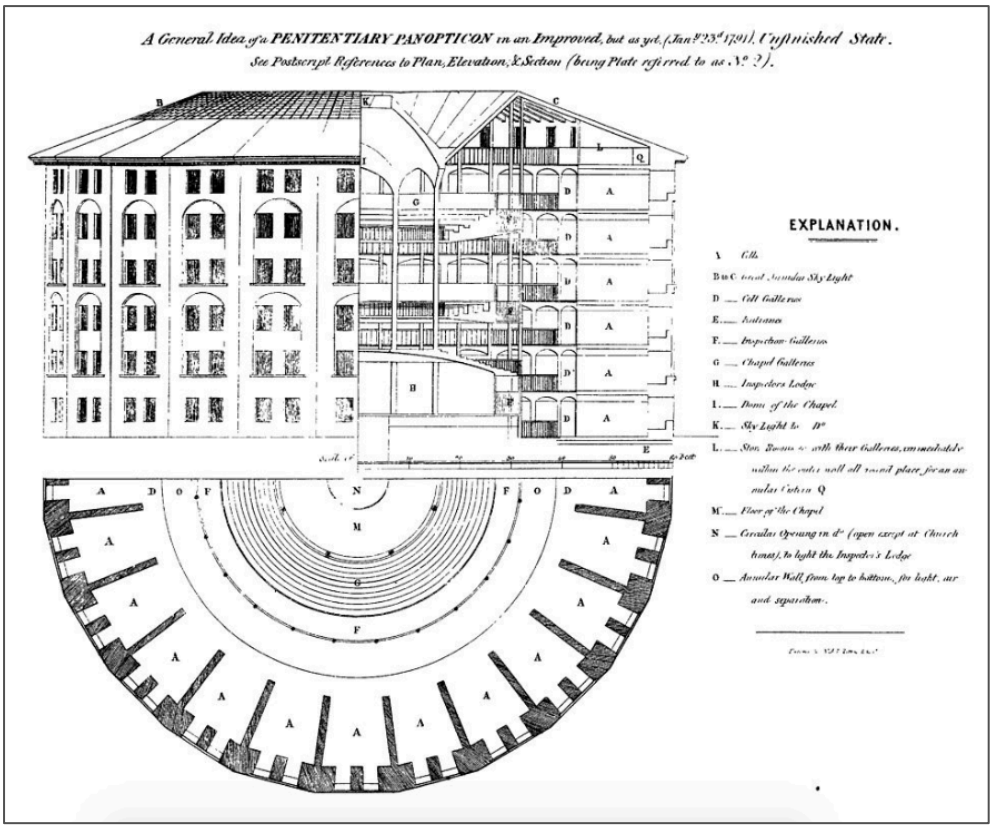
[32] Egen oversættelse af "personal dataveillance" (Clarke, 1988, s. 502).

[33] Egen oversættelse af "mass surveillance" (Clarke, 1988, s. 499).

[34] Fra det engelsk "The Inspection-house". Dette er undertiden oversat med "Opsynshus".

med hvilket Bentham udpegede den ide: "[...] that the persons to be inspected should always feel themselves as if under inspection, at least as standing a great chance of being so, yet it is not by any means the only one." (Bentham, 1843, s. 44).

Opsynsprincippet skulle materialiseres arkitektonisk i en præcist beskrevet cirkelformet bygningsstruktur med enkeltmandsceller, hvilket er illustreret på billede 2.[35]



Billede 2: Plantegning over Panoptikon (https://en.wikipedia.org/wiki/Willey_Reveley)

Panoptikon skulle endvidere i midten indeholde et observationstårn eller *the Inspector's lodge,* som Bentham omtaler dette (Bentham, 1843, s. 40). Fra dette observationstårn kunne overvågeren konstant holde øje med de indsatte, hvis ønsket. De overvågede kunne omvendt aldrig se overvågeren. Kernen i

[35] Det var Jeremy Benthams bror, Samuel Bentham, der fik og udviklende selve den arkitektoniske ide til Panoptikon.

Panoptikons virkemåde er den *tilsyneladende allestedsnærværelse* af overvågeren i kombination med, hvor ubesværet overvågerens virkelige tilstedeværelse er.

Hver indsat i Panoptikon eller andre institutioner[36] udformet efter samme princip kan nu analyseres individuelt: Man kan kategorisere og klassificere disse. Overvågningen bliver dermed en automatiseret og anonymiseret proces. Den konstante bevidsthed om, at overvågning måske finder sted i kraft af Panoptikons konstruktion, medfører, at der finder en særligt betydningsfuld proces sted: En internalisering af overvågningen i de overvågede subjekter, hvor den overvågede som minimum føler sig overvåget (Bentham, 1843, s. 44). Panoptikons funktion som overvågningsteknologi kan grundet internaliseringen af overvågningen i subjekterne ironisk nok også "opretholde" sig selv (Foucault, 1995, s. 201), og de overvågede subjekter oplever et mentalt fængsel. Ifølge den franske filosof Michel Foucault (1995) (1926-1984) skal Panoptikon ses som en repræsentativ kondensering af de overvågningsmekanismer, der er på spil "ude" i samfundet.

Foucault har uden tvivl bidraget med interessante perspektiver på overvågning. Foucault vil i afhandlingen blive anvendt til at belyse aspekter af overvågning, men hans ideer bør langt fra opfattes som udtømmende, når man vil indfange hele den kompleksitet, der kendetegner overvågning i dag. Der er også set forsøg på at udvide eller modernisere Panoptikon eksempelvis med Thomas Mathiesens term *Synopticon*, der beskriver de mange, der overvåger de få (Albrechtslund, 2008, s. 49).

Med hensyn til Panoptikon har Foucault desuden pointeret, at den vigtigste virkning heraf er, at de indsatte har den konstante bevidsthed om, at de muligvis bliver overvåget, uanset om de så rent faktisk bliver det eller ej (Foucault, 1995, s. 201). Der er altså tale om, at overvågningen har værdi, uag-

[36] Bentham nævner selv, at den arkitektoniske struktur og dermed også den grundlæggende ide i form af opsynsprincippet med fordel kan appliceres på skoler, hospitaler, fabrikker samt gale- og tvangsarbejdsanstalter (Bentham, 1843, s. 40).

tet om selve overvågningen egentlig finder sted (Clarke, 1988, s. 505; Foucault, 1995, s. 201, 204). Foucault udtrykker dette således:

> "Hence the major effect of the Panopticon: to induce in the inmate a state of conscious and permanent visibility that assures the automatic functioning of power. So to arrange things that the surveillance is permanent in its effects, even if it is discontinuous in its action [...]." (Foucault, 1995, s. 201).

Til trods for at ideen om Panoptikon er flere hundrede år gammel, synes den stadig at være en anvendelig og særligt væsentlig metafor for overvågning. Tilsvarende gælder det, at Foucaults genealogiske analyser[37] af de magtdynamikker, der her er på spil, stadig indfanger *nogle* af de relevante problematikker og centrale elementer i overvågning på et mere abstrakt niveau.

Man kan argumentere for, at disse tanker om overvågning, hvor den bærende ide er en overvågningsuafhængig overvågningseffekt, udpeger en central problemstilling ved overvågning af data. Den påvirkning, som potentiel eller reel overvågning medfører, er én af grundene til, at overvågning kan problematiseres og kritiseres. *Dataveillance* som overvågningsform er ikke videre transparent, og dermed gør i hvert fald nogle af de samme forhold sig gældende (Marx, 2002, s. 28-29). Clarke hævder endvidere, at masseovervågning kan lede til, at det enkelte individ oplever en ændring af eget selvbillede eller egen selvforståelse. Yderligere kan man opleve en: "[...] stultification of the independent spirit needed to meet the challenges of the future." (Clarke, 1988, s. 508).

Walter Peissl sondrer mellem overvågningens kortsigtede og langsigtede påvirkninger af individer og samfund (Peissl, 2003, s. 22). En kortsigtet påvirkning er tilpasning af individets opførsel, hvilket af Peissl benævnes mainstreaming. Det vil i praksis betyde, at de enkelte individer ikke opfører sig som "sig selv", men i stedet opfører sig, som de tror, de bør eller skal opføre sig. Denne ide findes også hos Jefferey Reiman (1995). Reiman argumenterer, at såfremt et individ observeres, vil dette individ helt naturligt identificere sig

[37] En genealogisk analyse anvendes til at stille spørgsmål ved den gængse opfattelse af sociale og filosofiske overbevisninger, og hvor denne opfattelse kommer fra.

med den observerendes perspektiv og gøre dette til sit eget. Resultatet er et såkaldt *double vision* med Reimans egen terminologi. *Double vision* betyder, at den observerede identificerer sig med den observerendes perspektiv og tilføjer dette perspektiv til sit eget. Ydermere fører *double vision* til, at den observerede vil handle anderledes end ellers (Reiman, 1995, s. 38).

Peissls og Reimans ideer kan føres tilbage til Foucault, der i forbindelse med overvågningens betydning behandler "den normaliserende sanktion"[38], hvor et af formålene er at korrigere og reducere afvigelser – at socialisere subjektet. Den normaliserende sanktion definerer de parametre, der er grundlaget for at bedømme subjektet (Foucault, 1995, s. 177-178). Et interessant kendetegn ved den normaliserende sanktion er, at det, der straffes, er af ligegyldig karakter i juridisk forstand og dermed ikke indfanges af dette traditionelle straffesystem. Derimod etableres der, hvad Foucault betegner en "understrafferet",[39] der enten godkender eller diskvalificerer bestemt adfærd (Foucault, 1995, s. 178).

Normalisering leder endvidere til oplevelsen af mistet autonomi for det enkelte individ. Dette synspunkt understøttes af Clarke, der har påpeget, at: "In general, mass dataveillance tends to subvert individualism and the meaningfulness of human decisions and actions, and asserts the primacy of the state." (Clarke, 1988, s. 508).

At overvågning har en socialiserende effekt og tillige påfører individerne et autonomi-tab, har en række problematiske implikationer i forhold til nutidens liberale, demokratisk styrede stater (Gavison, 1984; Regan, 1995). Sådanne stater bygger på en grundlæggende ide om, at individer er selvbevidste, frie og autonome størrelser, der selv kan og tør foretage det ønskede valg. Privathed kan være med til at fostre et tolerant samfund, der er præget af pluralisme og plads til individuel udvikling (Gavison, 1984, s. 369). Får det enkelte individ ikke muligheden for at udvikle sig, kan det have betydning for stat og sam-

[38] I den engelske oversættelse benævnes dette "normalizing judgement" (Foucault, 1995, s. 177).

[39] I den engelske oversættelse benævnes dette "infra-penalty" (Foucault, 1995, s. 222).

fund. Det er et grundlæggende problem for demokratiet som styreform, hvis individet ikke har rum til at udvikle sig som ønsket og til at tænke frit. Det indgående kendskab, som *dataveillance* kan give staten om individerne, skal med andre ord ikke udelukkende anskues som værende fordelagtigt for en stat. Dette er en simplificering. Der er tale om en polarisering i debatten omhandlende overvågning:

> "[...] in the context of government surveillance, civil libertarians depict the government as pursuing absolute power, while law enforcement officials blame privacy for child pornography and airplanes falling out of the sky." (Polonetsky & Tene, 2013, s. 26).

Samtidigt påpeger Polonetsky og Tene, at lige meget hvilke fordele det giver, vil privathedsfortalere ikke give køb på privathed. Omvendt vil fortalere for dataindsamling argumentere for, at privathed blot er en: "[...] afterthought in the pursuit of complete information." (Polonetsky & Tene, 2013, s. 26). Hvis denne polarisering bliver grundlaget for en diskussion, vil det være særdeles svært at handle.

Konsekvenserne af overvågning kan således få betydning for stat og samfund. En vis variation individerne imellem er en nødvendig betingelse for, at et samfund kan udvikle sig, men socialisering afstedkommer i praksis, at denne variation mindskes (Foucault, 1995; Peissl, 2003, s. 22). Peissl argumenterer for, at såfremt overvågning leder til et stop i samfundsudviklingen, så betyder det, at eksempelvis terrorister har opnået, hvad de ønskede i første omgang (Peissl, 2003, s. 23).

Man kan diskutere, om det eneste terrorister har som formål, er at stoppe samfundets udvikling, eller om de også har andre mål? Om ikke andet har terrorister, hvis de kan stoppe samfundets udvikling, i hvert fald opnået dele af deres mål. Det er interessant i den forbindelse, at vi overvåger med opretholdelse af offentlig sikkerhed som mål og dermed også med ønsket om at undgå terrorismens indvirkning på samfund og individer. Ironisk nok kan vi således modsat vores ønske ende med det resultat, som terrorister ønskede i første omgang (Peissl, 2003, s. 22).

Til trods for at ovenstående konsekvenser af overvågning er yderst problematiske, vil jeg stadig fastholde den grundlæggende antagelse, som er præsenteret indledningsvist i denne introduktion, at overvågning ikke nødvendigvis kan karakteriseres som værende et onde eller noget uønsket i sig selv. Problemstillingerne, der knytter sig til overvågning og teknologi, bestemmes i det væsentlige af, hvordan overvågningen udføres og anvendes i praksis, og i mindre grad af overvågningen *per se* (Clarke, 1988, s. 498-499).

I kapitel 3., *Overvågning og implikationer heraf,* demonstreres det desuden, hvordan overvågning er et komplekst begreb, der kan anvendes i mange sammenhænge med forskellige intentioner og formål.

1.5. INFORMATIONEL PRIVATHED

Tab af privathed er én af grundene til, at overvågning problematiseres. Litteraturen om privathed vidner om en betydelig diversitet i måderne at tilgå og begrunde privathed. Nogle afviser ligefrem værdien af privathed. I den klassiske artikel "The Right To Privacy" (1984)[40] påpeger Judith Jarvis Thomson, at: "Perhaps the most striking thing about privacy is that nobody seems to have any clear idea what it is." (Thomson, 1984, s. 272). Thomson, der har et reduktionistisk syn på privathed, mener, at privathed i virkeligheden kan reduceres til rettigheder af andre typer. Retten til privathed er med andre ord blot afledt fra andre rettigheder, og ifølge Thomson kan det forkerte i at krænke privathed, forklares uden nogensinde at nævne privathed (Thomson, 1984, s. 287). Denne reduktionistiske tilgang kan eksemplificeres med en situation, hvor en person i eget hjem har gemt et pornografisk fotografi, hvor personen selv er afbildet. En anden person finder fotografiet og betragter dette. Der er her ikke tale om en krænkelse af privathed ifølge Thomson. Det er derimod et spørgsmål om, at ejendomsretten til billedet er krænket (Thomson, 1984, s. 287). Krænker man en persons privathed, krænker man i virkeligheden blot andre mere basale rettigheder.

[40] Originalkilden blev publiceret første gang i 1978.

Rachels har fremhævet det problematiske i at ville sidestille ejendomsret og ret til privathed (Rachels, 1984, s. 297). Anerkender man, at privathed eksisterer, og at retten til privathed ikke kan reduceres til en ejendomsret, så forekommer der også at være forskel på den interesse, man har i sin krop, og den interesse, man har i sin bil (Rachels, 1984, s. 297). Argumentet kan yderligere styrkes ved at bringe et citat fra Floridi, der har anført, at:

> ''My'' in ''my information'' is not the same ''my'' as in ''my car'' but rather the same ''my'' as in ''my body'' or ''my feelings'': it expresses a sense of constitutive belonging, not of external ownership, a sense in which my body, my feelings and my information are part of me but are not my (legal) possessions." (Floridi, 2005, s. 195).

Hvis man ser på privathed, som Floridi fremstiller det, hvor der er et analogt forhold mellem *"my"* og *"my body"* og *"my"* og *"my information"*, så forekommer Rachels argument for, at der er forskel på ens krop og ens bil, styrket.

Der har været megen modstand mod Thomsons kritiske og privathedsreducerende perspektiv. Min påstand er, at det rent intuitivt forekommer forkert at hævde, at hvis nogen kigger på et pornografisk billede af en anden, så er det *udelukkende* et spørgsmål om, at ejendomsretten til et billede er krænket. Det synes, hvad angår ovenstående eksempel, at være rimeligt at hævde, at også noget, der har at gøre med privathed, krænkes.

Privathed rubriceres oftest som en instrumentel værdi, der knytter sig til det enkelte individ (Kupfer, 1987, s. 81), og som således har betydning for mere fundamentale rettigheder. Privathed har blandt andet været begrundet instrumentelt i forhold til retten til at være alene (Warren & Brandeis, 1984), hvilket nogle mener, er en forudsætning for såvel intimitet (Fried, 1984; Gerstein, 1984a) som muligheden for at opretholde sociale relationer (Rachels, 1984).

Kontrol med information om en selv har været anset for en betingelse for privathed (Fried, 1984; Warren & Brandeis, 1984). Reiman har i en kritik af privathed som kontrol påpeget, at det ikke er muligt at opretholde kontrol over information. Han har forsvaret privathed som et spørgsmål om begrænset

adgang til information (Reiman, 1995). Privathed også har været begrundet under henvisning til retten til autonomi (Kupfer, 1987, s. 82).

Privathed anses, som det tidligere er nævnt i afhandlingen, ikke udelukkende som et gode for individet, men som en værdi der er vigtig for en stats og et samfunds virke som helhed. Statens og samfundets udviklingsmuligheder beror på, at individet kan udvikle sig frit, hvilket igen forudsætter privathed. Det velfungerende demokrati behøver også privathed. Gavison har endvidere argumenteret for, at politikere har brug for privathed til at udvikle deres politik (Gavison, 1984, s. 370). Individer i en stat har brug for privathed for frit at kunne udvikle egne tanker og ideer, hvilket er fundamentet for demokratiet.

Såfremt det anerkendes, at privathed har værdi for såvel individet som for staten og samfundet, vil konsekvensen være, at der bør gives betragtelig vægt til den indfaldsvinkel, at privathed bør prioriteres, når nye love skal formuleres (Regan, 1995, s. 214). En sådan tilgang vil også være et stærkt incitament til at udvikle ny teknologi, der ikke kun har offentlig sikkerhed for øje, men også anerkender vigtigheden af privathed. En sådan tankegang vil kunne finde plads i et liberalt demokrati, hvor individets ret til privathed og autonomi vægtes højt.

Privathed, og hvad dette begreb dækker over, har gennem tiden ændret sig drastisk (Moor J. H., 1997, s. 30). Denne udvikling kan ses som en naturlig proces, der er en følge af ydre, samfundsmæssige omstændigheder. I dag er såkaldt *informationel privathed* blevet særlig aktuel som konsekvens af de voksende mængder *greased data*, vi har til rådighed, og som følge af det forhold, at privathed i høj grad informationsberiges (Moor J. H., 1997, s. 30; Tavani, 1999, s. 138). Informationel privathed, der er den form for privathed, der er i fokus i afhandlingen, er af Clarke defineret som: "[...] the interest an individual has in controlling, or at least significantly influencing, the handling of data about themselves." (Clarke, 2013). Hermed illustreres det syn, at privathed handler om *kontrol* med data i et eller andet omfang, hvilket eksempelvis er forsvaret af Fried (Fried, 1984).

Som en konsekvens af at data i dag er *greased*, er det ifølge Moor ikke muligt at kontrollere sin informationelle privathed fuldstændigt, til trods for at det ifølge Moor er ønskværdigt (Moor J. H., 1997, s. 31). Derimod må man tilstræbe at begrænse adgangen til data. Kun de rette mennesker på de rette tidspunkter skal have adgang hertil (Moor J. H., 1997, s. 31). Hvorvidt man kan tale om, at privatheden bliver kompromitteret, er således ikke længere et spørgsmål om informationen i sig selv, men et spørgsmål om, hvorvidt informationen er passende eller ikke i en given kontekst eller zone, og om måden, hvorpå informationen bevæger sig mellem mennesker (Moor J. H., 1997; Nissenbaum, 2010).

Problemstillinger, der knytter til sig informationel privathed og sikkerhedsteknologi, drejer sig typisk om måden, hvorpå indsamling, anvendelse og videregivelse af information foregår, og om, at denne informationsbehandling sker uden at personen, som informationen angår, er vidende herom og/eller har mulighed for at begrænse dette (Cavoukian, 1998, s. 10; Tavani, 1999, s. 138).

Data, der frivilligt gøres mere eller mindre offentligt tilgængelige på sociale medier, kan i dag anvendes som led i en analyse på en måde, som oprindeligt ikke var tiltænkt eller forudset. Dette forhold demonstreres af det omtalte Twitter-eksempel (Gerber, 2014). Den situation åbner samtidigt også for diskussionen om privathed i spændingsfeltet mellem den private og den offentlige sfære, hvilket Nissenbaum har behandlet og indfanget med det analytiske begreb *kontekstuel integritet*[41]. Hermed introduceres ideen om informationel privathed som et kontekstrelativt fænomen (Nissenbaum, 2010). Nissenbaum introducerer en række redskaber, der kan bruges til at analysere og forklare, hvorfor privathedsproblemer opstår. Jeg vender tilbage til disse redskaber i kapitel 4., *Informationel privathed.* At opfatte privathed som et kontekstrelativt fænomen kan være særligt hensigtsmæssigt, når man ønsker at forklare kernen i de problemer, der kan opstå ved at høste data online i én kontekst og anvende dem i en anden. Et eksempel kan illustrere pointen.

[41] Egen oversættelse af den engelske betegnelse ”contextual integrity” (Nissenbaum, 2010)

Brugere bidrager selv til egen afprivatisering, når de eksempelvis lægger data på sociale medier. I nogle tilfælde lægger brugere information på sociale medier, der er offentligt tilgængelige for alle med en Facebook-konto. Man kan forestille sig en bruger, der ofte opdaterer Facebook om sin gøren og laden ved at "checke ind" på sin arbejdsplads, i fitnesscenteret, på restauranter, hjemme hos sig selv og hos venner og bekendte med det formål at lade vennerne vide, hvad pågældende bruger foretager sig. Det kan virke kontraintuitivt at argumentere for, at privathed har betydelig værdi, hvis man samtidigt selv skaber et offentligt tilgængeligt spor i kraft af information om sig selv på et socialt medie. Her kan den kontekstrelative privathedsforståelse dog bringes i spil som en forklaringsmodel, idet disse informationer er uproblematiske i henseende til privathed inden for den kontekst, de er tiltænkt. Flytter man informationerne ud af denne kontekst, kan de derimod overskride en grænse i forhold til privathed.

1.5.1. KRITISKE PERSPEKTIVER PÅ PRIVATHED

Privathed har som nævnt mødt modstand med forskellige begrundelser. Richard A. Wasserstrom (1984)[42] har med afsæt i begrebet *modkultur*[43] fremstillet en kritik af privathed. Modkultur er Wasserstroms alternative perspektiv på privathed, hvormed han mener at kunne demonstrere, at privathed skal opfattes anderledes, end vi gør det. Wasserstrom anfører, at privathed bygger på en kulturelt betinget antagelse om, at det er pinligt, hvis eksempelvis intim information om en person bliver kendt af andre, end personen selv har ønsket (Wasserstrom, 1984, s. 330). Ifølge Wasserstrom er dette: "[...] a significant feature of our culture [...] What I'm less sure about is the question of whether is it necessarily a desireable feature of a culture." (Wasserstrom, 1984, s. 330). Wasserstrom hovedpointe er, at mennesker ville være bedre tjent med blot at være, hvem de i virkeligheden er, og ikke skjule det, som vi mener er skamfuldt, med mindre det foregår i et privat domæne (Wasserstrom, 1984, s. 330). Tillader vi det, vil det gå op for os, at alle andre har samme ønsker og fantasier

[42] Originalkilden blev publiceret første gang i 1978.

[43] Egen oversættelse af "counterculture" (Wasserstrom, 1984, s. 330)

– vi bør slet ikke være skamfulde i forhold hertil. Ifølge Wasserstrom er det, der er skamfuldt, blot et udtryk for et kulturelt fænomen – en kulturel norm. Der er intet, der hindrer, at personer kan have sex i offentligheden, ganske som de kan spise et måltid offentligt – udover socialt konstruerede kulturelle normer (Wasserstrom, 1984, s. 330-331).

Ligesom Wasserstrom diskuterer Anton Vedder blandt andet privathed i lyset en norm (Vedder, 2011). Vedder har stillet spørgsmålstegn ved, om vi skal "[...] applying privacy norms or changing the taboo?" (Vedder, 2011, s. 23), når det kommer til det, som vi beskytter med netop privathed – eksempelvis vores nøgne krop, sexliv og samtaler om intime detaljer og relationer. Kommer sådanne informationer i hænderne på nogen, som de ikke var tiltænkt, kan man føle sig sårbar og miste status og omdømme (Vedder, 2011, s. 23).

Privathed kan ydermere kritiseres fra et feministisk synspunkt, idet privathed kan blive et skjul for mænd med voldelige og dominerende tendenser (DeCew, 2013). Er privathed en måde at sikre, at omverdenen ikke kan få kendskab til det, der sker i hjemmet, så må løsningen være at operere med langt større transparens eller helt ophæve privatheden, hævder feministerne. Det er dog ikke en hensigtsmæssig løsningsmodel ikke at tillade privathed, idet det vil have særdeles betydningsfulde omkostninger for samfundet som helhed. Den feministiske kritik af privathed er for så vidt reel nok, idet privathed netop kan udgøre et skjul for uretmæssig adfærd overfor kvinder. Dog forekommer ideen med at fjerne muligheden for at opretholde privathed ikke at være den mest hensigtsmæssige løsning (Allen, 2011).

Man kan i forlængelse af ovenstående også påpege, at kvinder ligesom mænd kan "drage fordel" af privathed i forhold til at udøve vold eller dominerende tendenser eksempelvis i hjemmet. Dermed mener jeg, at den feministiske kritik i den form, som jeg kort har skitseret her, ikke nødvendigvis har sammenhæng med kvindeundertrykkelse. Problemstillingen er ikke særlig i feministisk forstand. Jeg anerkender dog, at privathed kan være et problem for kvinder.

Et andet område, der kan give anledning til, at kritik af privathed rejses, er kriminalitetsforebyggelse. Privathed er det perfekte skjul for kriminelle aktiviteter og giver mulighed for *free-riding* (van den Hoven, 1997, s. 33). Der kan eksempelvis være tale om, at individer modtager sociale ydelser, som de ikke er berettiget til. Høj grad af privathed hæmmer kontrol med sociale ydelser og øger dermed risikoen for socialt bedrageri. Hvis man derimod samkører data, vil man kunne opdage den slags snyd. Et eksempel herpå stammer fra Italien. Man samkørte data om personer, der fik sociale ydelser på grund af blindhed, og data om personer, der for nylig havde fået et kørekort, for at finde personer, der foretog *free*-riding (van den Hoven, 1997, s. 33). Muligheden for at bekæmpe kriminel aktivitet, herunder specifikt terror, var også begrundelsen for at indsamle metadata i forbindelse med Logningsdirektivet (Institut for Menneskerettigheder, 2015, s. 15).

Muligheden for at kunne stoppe eller i hvert fald begrænse, at individer udfører kriminel aktivitet, kan være en konkret begrundelse for at øge overvågning af data. Det er fordelene for fællesskabet – samfundet som helhed - der her er i centrum (van den Hoven, 1997, s. 33). Rationalet er, at hvis vi tillader mindre privathed, så får vi mere sikkerhed. Betragter man omvendt spørgsmålet om, hvorvidt vi skal bekæmpe *free-rider*-problematikken og kriminel aktivitet med udgangspunkt i et liberalt perspektiv, vil man give fællesskabsfortalerne ret i, at staten skal blande sig. Forskellen mellem de to perspektiver består i, *i hvilken grad* man skal tillade, at statslige organer blander sig.

Som det fremgår af ovenstående introduktion til privathed, er der særdeles forskellige begrundelser for, hvorfor privathed har en værdi, ligesom der er argumenter for, at vi bør opgive privatheden. En grundlæggende antagelse i denne afhandling er, at privathed er værdifuldt. Det er en del af grundlaget for, at det overhovedet er nødvendigt at diskutere, hvordan man forener privathed og offentlig sikkerhed i teknologi. Var privathed ikke værdifuld, ville denne diskussion være unødvendig.

Privathed er som værdi funderet i en række retskilder og er navnlig i EU et velreguleret, juridisk område. I EU-sammenhæng sker denne regulering på

nuværende tidspunkt primært ved det såkaldte Databeskyttelsesdirektiv fra 1995 (Direktiv 95/46/EF) , hvor det centrale element er beskyttelse af personhenførbare data, men samtidig at muliggøre udveksling af personoplysninger mellem lande i EU (Europa-parlamentet og rådets direktiv, 1995). Dertil kommer en række andre grundlæggende principper, rettigheder og konventioner (Menneskerettighedskonventionen, Den Europæiske Unions Charter om Grundlæggende Rettigheder, Code of Fair Information Practices og The OECD Privacy Framework.)

Som det gerne skulle stå klart på nuværende tidspunkt, så sigter nærværende afhandling mod at behandle spændingen mellem informationel privathed og offentlig sikkerhed i den sikkerhedsteknologi, der bruges til at overvåge data. I afhandlingen betragtes denne problemstilling i et etisk perspektiv. Dermed rejser spørgsmålet sig om, hvori etikkens berettigelse består, hvis vi netop har en velreguleret beskyttelse af data i EU? Senere i afhandlingen præsenteres og diskuteres tre begrundelser herfor. Der argumenteres blandt andet for, at de værdibaserede design-tilgange, som jeg diskuterer og vurderer i forhold til sikkerhedsteknologi, sigter mod et andet niveau end EU-lovgivningen. EU-lovgivningen er kendetegnet ved at beskæftige sig med de personer, der behandler data. De værdibaserede tilgange, der inddrages i afhandlingen, har derimod fokus på hele design-processen fra start til slut og på at understøtte eller hindre bestemt brug af teknologi.

1.6. INDIVIDET I STATEN

Det enkelte individ er en del af en statskonstruktion, hvorfor man kan argumentere for, at individet ikke kan kræve *absolut* privathed og kontrol over egne informationer (Blume, 2000, s. 5). Konkret i forhold til afhandlingen er ideen, at adgang til informationer ved hjælp af *dataveillance*-teknikker såsom analyse af data kan lede til mere national sikkerhed (Thuraisingham, 2002, s. 1). Ideen om, at individet afgiver noget og modtager noget andet, kommer fra social kontraktteori (Hobbes, 2001; Hume, 1999; Locke, 2003). Social kontraktteori vil jeg diskutere i kapitel 6., *Offentlig sikkerhed.*

Overvågning af enkelte individer og grupper af individer er et væsentligt våben i kampen mod kriminel aktivitet. Clarke noterer sig også, at det må anses for rimeligt, at nogle mennesker overvåges. Personer, der er involveret i terror eller organiseret kriminalitet, kan være eksempler herpå. De fleste mennesker vil nok erklære sig enige i, at overvågning af sådanne personer bør finde sted (Clarke, 1988, s. 499). Samtidigt med at individer næppe kan forvente absolut privathed, kan en stat dårligt kræve en ubegrænset adgang til informationer, der knytter sig til det enkelte individ, selvom disse informationer indsamles i sikkerhedsøjemed. Som det blev gjort klart indledningsvist og i foregående afsnit, vil det heller ikke være en gavnlig praksis, idet staten herved skaber en lang række problemstillinger for ikke alene individet, men også for samfundet og staten selv. Samtidigt kan man også argumentere for, at: "[...] governments must be held to a higher standard for the collection and use of personal data than private actors." (Executive Office of the President, 2014, s. 10). Staten og individet bliver i nærværende afhandling opfattet som to parter, der begge kan drage fordel af både offentlig sikkerhed og informationel privathed.

Opretholdelse af offentlig sikkerhed ved brug af *big data* som grundlag for *dataveillance* kan medføre et tab af privathed, hvis informationel privathed og offentlig sikkerhed ikke er forenet på en hensigtsmæssig måde i teknologi. Sådan behøver det imidlertid ikke nødvendigvis at forholde sig, og : "If there is the will to do so, the technological and organizational security solutions can be designed to minimize the infringement of privacy." (PRISE, s. 2). Ofte sker der dog det, at man ignorerer privathed, imens man designer en given teknologi, og afslutningsvis tilføjes privathedsbeskyttelse som en slags *add-on* (Klitou, 2014, s. 264; PRISE, s. 3; Wang & Kobsa, 2008, s. 18). Jeg argumenterer i afhandlingen for, at informationel privathed og offentlig sikkerhed begge er fordelagtige værdier for både stat og individ. Dermed gælder det, at en løsning på den "konflikt", som eksisterer mellem informationel privathed og offentlig sikkerhed, er nødvendig.

1.7. VÆRDIER I DESIGN: VALUE SENSITIVE DESIGN OG PRIVACY BY DESIGN

I afhandlingen diskuteres den spænding, der kan opstå mellem værdierne informationel privathed og offentlig sikkerhed i sikkerhedsteknologi. Der argumenteres for, at såvel informationel privathed som offentlig sikkerhed har en signifikant betydning for såvel stat som individ, hvorfor det er fordelagtigt at designe teknologi, der kan fremme begge værdier.

Til at realisere værdier i teknologi findes forskellige tilgange, hvoraf jeg i nærværende afhandling vil beskæftige mig med VSD (Albrechtslund, 2007; Friedman & Kahn, 2003; Friedman, Kahn, & Borning, 2001; van den Hoven, 2007; van den Hoven & Manders-Huits, 2012) og PbD (Cavoukian, 2011; Cavoukian, 2012c). VSD og PbD er netop kendetegnet ved at bygge på et princip om, at værdier skal tages i betragtning igennem hele designprocessen fra start til slut (Cavoukian, 2011; Friedman & Kahn, 2003, s. 1186). I lyset af afhandlingens genstandsfelt er denne måde at tilgå de etiske hensyn også yderligere aktualiseret, idet Wang og Kobsa bemærker, at:

> "Privacy needs to be treated as a first-class requirement from the early onset in the design of an information system since, like for security and usability, it is extremely difficult if not impossible to "retrofit" a completed system to make it more friendly." (Wang & Kobsa, 2008, s. 18).

PbD har netop det formål konkret at sikre, at privathed bliver taget med i designovervejelser allerede fra starten af et designprojekt i stedet for at blive "skruet på" efterfølgende (Klitou, 2014, s. 264). PbD sigter specifikt mod værdien privathed og består af syv grundlæggende principper (Cavoukian, 2011). Den grundlæggende præmis i PbD er, at det er mere effektivt og hensigtsmæssigt at tage privathed i betragtning allerede i forbindelse med design og fremstilling af teknologi, end det er at lade det være op til brugerne at fremme en sådan værdi. PbD har således ikke brugere af teknologi i fokus, men derimod designere og producenter (Cavoukian, 2011; Klitou, 2014).

VSD kan med udgangspunkt i menneskelige værdier anvendes til at kvalificere designprocesser og er kendetegnet ved at advokere for, at man bør have et

bredere perspektiv på, hvad vellykket teknologisk design er (Nissenbaum, 2001, s. 118; van den Hoven & Manders-Huits, 2012, s. 477-478). VSD er en tredelt iterativ metodologi, som kan anvendes til proaktivt at påvirke en designproces fra start til slut. VSD tager afsæt i et interaktionsperspektiv, hvilket betyder, at de egenskaber, en teknologi designes med, vil undersøtte eller undertrykke bestemte værdier, samtidigt med at den faktiske brug af en teknologi afhænger af de personer, der anvender teknologien og deres mål hermed (Friedman, Kahn, & Borning, 2006, s. 360).

Nissenbaum mener, at en bredere forståelse af teknologi, hvor sociale, etiske og politiske værdier også indregnes, er nødvendig (Nissenbaum, 2001, s. 118). De teknologiorienterede og funktionelle succeskriterier, man ofte ser, kan dog forklares med, at det er ingeniører, der selvstændigt udvikler ny teknologi, ligesom deres baggrund betyder, at eksempelvis etiske værdier ikke tages i betragtning. Et eksempel er NSA's overvågningssystemer, som Snowden afslørende tilbage i 2013. Systemerne er blevet kritiseret for ikke at tage etiske værdier som for eksempel privathed i betragtning (Timmermans & Mittelstadt, 2014, s. 1-2).

Vellykket implementering af værdibaseret design indebærer dog, at det ikke er muligt at klare sig med udelukkende tekniske eller humanistiske kundskaber i designarbejdet, men derimod er der brug for et samspil mellem disse forskellige vidensdomæner (Flanagan, Howe, & Nissenbaum, 2008, s. 324-225). Med andre ord bør man i langt højere grad arbejde interdisciplinært (Nissenbaum, 2001, s. 120). Ofte er tekniske og humanistiske/sociale discipliner dog skarpt opdelte fagligheder, hvilket særligt tydeligt kommer til udtryk i den måde, de akademiske fagområder traditionelt set er opdelt indenfor universitetsverdenen (Flanagan, Howe, & Nissenbaum, 2008, s. 324-225). En mindre rigid adskillelse af fagområder er derfor en fundamental nødvendighed for at muliggøre vellykket værdibaseret design i praksis.

Proaktivitet er et centralt element i PbD og er eksplicit nævnt i det første af de syv grundlæggende principper, som PbD hviler på (Cavoukian, 2011). Med PbD ønsker Cavoukian, at værdien privathed proaktivt væves ind i teknologi-

en og samtidigt også direkte i selve operationaliseringen heraf. Som eksempler kan nævnes forretningsprocesser, praksisser og ledelsesstukturer (Cavoukian, 2012c). Van den Hoven beskriver en lignende ide, *front-loading ethics* [44], hvormed han refererer til en holistisk tanke om, at man skal foregribe de etiske problemstillinger, der kan opstå i forbindelse med teknologidesign, når eksempelvis it-arkitektur, krav, specifikationer, standarter og protokoller skal udarbejdes (van den Hoven, 2007, s. 70). Tankegangen her står i kontrast til tidligere tiders reaktive måde at gribe den etiske tænkning an på.

Inden for den engelske og amerikanske tradition tog etikken i det tyvende århundrede typisk sit udspring i en analytisk, metaetisk tilgang. Senere hen blev professionelle filosoffer mere interesserede i anvendt etik, hvor populære og velkendte, normative teorier som utilitarisme, pligtetik og dydsetik blev appliceret på problemstillinger i specifikke situationer for at bestemme, hvordan vi bør handle (van den Hoven, 2007, s. 70-71). Helt frem til sidste del af det tyvende århundrede blev teknologi endvidere typisk anset for at være værdineutral, hvor teknologi betragtedes som et instrument for menneskelige aktiviteter (Manders-Huits, 2011, s. 272). Van den Hoven argumenterer for, at der i dag er ved at ske en designdrejning (van den Hoven, 2007, s. 71; van den Hoven, 1997). Rationalet er, at man allerede i designfasen forsøger at understøtte bestemt brug og hindre anden brug. Dog anerkender fortalere for VSD det forhold, at der ikke kan trækkes en ensrettet linje fra udvikling til brug, idet den person, der anvender en teknologi, også har indflydelse herpå. Der anlægges således et interaktionsteknologisk perspektiv på forholdet mellem teknologi, menneske og værdi.

1.7.1. UDFORDRINGER: VALUE SENSITIVE DESIGN OG PRIVACY BY DESIGN

Til trods for at såvel VSD og PbD er anerkendte metoder, knytter der sig en række problemstillinger til brugen af dem. Gürses et al (2011) peger eksempelvis på, at PbD-tilgangen er for vagt formuleret, hvorfor det aldrig bliver klart, hvordan denne strategi kan appliceres i en egentlig ingeniørpraksis (Gürses, Troncoso, & Diaz, 2011). Albrechtslund og Manders-Huits påpeger, at

[44] Begrebet er ikke oversat, da der ikke findes en passende dansk betegnelse.

VSD mangler en fundamental diskussion af bagvedliggende, normativ, etisk teori (Albrechtslund, 2007, s. 67; Manders-Huits, 2011, s. 282-283).

Friedman og Kahn har i forbindelse med VSD beskrevet en række værdier, hvoraf de fleste er hentet fra traditionelle, moralfilosofiske teorier som pligtetik og utilitarisme (Friedman & Kahn, 2003, s. 1187). Værdierne udgør tilsammen en ufuldstændig liste, der dog har givet Le Dantec et al (Le Dantec, Poole, & Wyche, 2009) grund til at mene, at VSD kan forbedres, hvis de etiske værdier er mindre præcist beskrevet, så værdierne alene styres af den specifikke kontekst, et givent projekt befinder sig i. Samtidigt efterlyses det af samme forfattere, at selve den tredelte metodologi, som udgør VSD, beskrives mere præcist (Le Dantec, Poole, & Wyche, 2009).

VSD tager afsæt i et interaktionsperspektiv på spørgsmålet om, hvordan værdier og teknologi indbyrdes integreres. Hermed anerkendes det, at designet af en teknologi har betydning for senere anvendelsesmuligheder, der dog også afhænger af de personer, der anvender teknologien (Friedman & Kahn, 2003, s. 1179). Personer vil have varierende formål med at anvende en teknologi, og brugen sker ikke altid på den måde, designeren oprindeligt havde tænkt. Således afvises et teknologideterministisk syn på forholdet mellem værdier og teknologi.

VSD og PbD repræsenterer en proaktiv tilgang til at realisere værdier i teknologi, men man må overveje, om denne fremgangsmåde er hensigtsmæssig, hvis der alligevel ikke eksisterer et deterministisk forhold mellem teknologiens design og anvendelsen i praksis. Albrechtslund (2007) har påpeget dette problem og anfører, at:

> "[...] it must be determined what can actually be predicted – functionally and ethically – in the design process, what would be an informed guess, and, finally, what is simply beyond the knowledge of the designers." (Albrechtslund, 2007, s. 68)

Til trods for at det er muligt at udpege problemstillinger ved både VSD og PbD, gør det sig gældende for begge tilgange, at de er anerkendte, men samtidigt særdeles omdiskuterede (Albrechtslund, 2007; Cavoukian, 2011; Friedman & Kahn, 2003; Klitou, 2014; Le Dantec, Poole, & Wyche, 2009; Manders-Huits,

2011; van den Hoven, 2007). Da *dataveillance* og *big data* vinder frem, er det relevant at undersøge, om tilgangene netop kan afhjælpe spændingen mellem informationel privathed og offentlig sikkerhed i forbindelse med sikkerhedsteknologier. I nærværende afhandling vil det i kapitel 8., *Realisering af værdier i design,* blive diskuteret og vurderet, hvorvidt tilgangene er anvendelige til at arbejde med værdierne informationel privathed og offentlig sikkerhed i sikkerhedsteknologi.

2. AFHANDLINGENS FUNDAMENT OG STRUKTUR

2. AFHANDLINGENS FUNDAMENT OG STRUKTUR

Nærværende afhandling er et it-etisk projekt, hvilket jeg vil uddybe nærmere i dette kapitels afsnit 2.1., *Afhandlingens it-etiske fundament.* Dernæst vil jeg påpege, hvorledes afhandlingen adskiller sig fra anden forskning, og hvorfor jeg finder, at projektets bredde er en styrke. Efterfølgende afgrænses afhandlingen i forhold til øvrige discipliner og relaterede problemstillinger. Ydermere findes der i afsnit 2.3., *Konventioner i afhandlingen,* en præcisering af en række begreber, efter hvilke principper oversættelser er foretaget osv. Til slut i nærværende kapitel er der en læsevejledning med introduktion af de enkelte kapitler. Her tydeliggøres det, hvorledes kapitlerne tilsammen belyser afhandlingens hovedtema, nemlig spændingen mellem informationel privathed og offentlig sikkerhed, når udvalgte sikkerhedsteknologier anvendes af staten.

2.1. AFHANDLINGENS IT-ETISKE FUNDAMENT

Grundlæggende er afhandlingen et teoretisk, it-etisk projekt. Computeretik er i James Moors klassiske artikel "What is Computer Ethics?" (1985) defineret som:

> "[...] the analysis of the nature and social impact of computer technology and the corresponding formulation and justification of policies for the ethical use of such technology." (Moor J. H., 1985, s. 266).

Moor anvender termen computeretik. Begrebet computer her skal forstås bredt og omfatter computere og associeret teknologi. Moor inkluderer således både software og hardware (Moor J. H., 1985, s. 266). De sikkerhedsteknologier, som behandles i afhandlingen, er eksempler på software. I afhandlingen anvendes termen it-etik om det, Moor kalder computeretik.

Moor påpeger om it-etik, at et af de forhold, der er med til at gøre dette område særligt, er, at man i forhold til it-etiske problemstillinger kan tale om såkaldt *begrebslig forvirring*[45]. Begrebslig forvirring betyder, at det er uklart, hvad et bestemt begreb egentlig dækker over (Moor J. H., 1985, s. 266). Umid-

[45] Egen oversættelse af "conceptual muddle" (Moor J. H., 1985, s. 266).

delbart kan det forekomme klart, hvad et givet begreb betyder, men mere grundig refleksion vil afsløre, at det ikke nødvendigvis er tilfældet. Et simpelt eksempel på en sådan begrebslig forvirring er en e-mail. Her må man afklare, hvorvidt en e-mail er ækvivalent med et "gammeldags" brev. Er en e-mail blot et brev i digitaliseret form, eller er der en række forhold, der betyder, at en e-mail ikke kan sidestilles med et brev?

I nærværende afhandling kan begrebslig forvirring komme til udtryk i forbindelse med *dataveillance*. Er *dataveillance* en forandring af begrebet overvågning, eller er *dataveillance* blot det samme som traditionel overvågning? Man kan i den forbindelse argumentere for, at vi i dag kan overvåge på en ny måde og via nye medier, men overvågningens grundtanke må siges at være den samme som tidligere. Mulighederne for overvågning har dog forandret sig og er tiltaget dramatisk i antal og omfang.

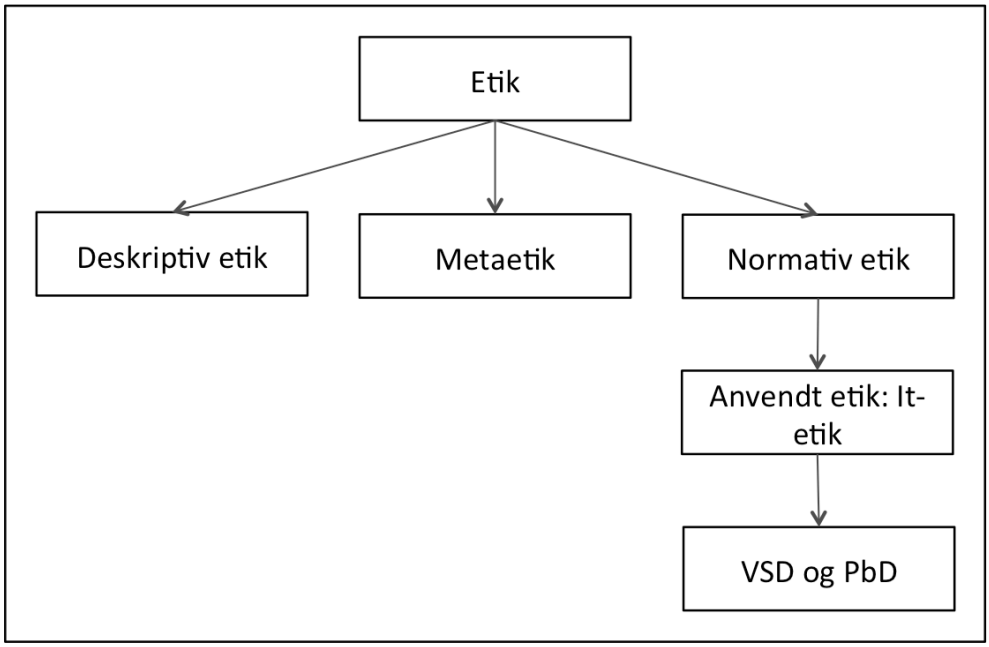
Begrebslig forvirring er nært forbundet med det, som Moor har navngivet *politisk tomrum*[46]. Et politisk tomrum vil sige, at der mangler anvisninger for, hvordan en given teknologi bør anvendes og i hvilket omfang, idet teknologier kan give os nye eller forandrede handlemuligheder (Moor J. H., 1985, s. 266). Dette er også med til at belyse, hvorfor man overhovedet skal diskutere den problemstilling, som afhandlingen tematiserer. Her er der ikke kun tale om en juridisk gennemgang af en given problemstilling, men også en etisk diskussion. Yderligere begrundelser herfor findes i kapitel 5., *Databeskyttelse: Retskilder og etikkens berettigelse*.

Der er forskellige måder, hvorpå man kan tilgå it-etiske spørgsmål med henblik på at foreskrive, hvorledes man bør handle i en given situation. Én måde er at søge at applicere traditionel moralfilosofisk teori som utilitarisme eller pligtetik på en given problemstilling. At anvende en sådan tilgang til afhandlingens problemstilling forekommer imidlertid problematisk, idet anvendelse af traditionel moralfilosofi ikke tilbyder en systematisk måde, på hvilken man kan arbejde med værdier i teknologi, og heller ikke systematisk tilgang til, hvordan man kan designe teknologi med henblik på at løse værdikonflikter.

[46] Egen oversættelse af "policy vacuum" (Moor J. H., 1985, s. 266).

Traditionel moralfilosofi fokuserer ofte på en enkelt værdi ad gangen (Friedman & Kahn, 2003, s. 1184). Eksempelvis kan der være tale om et specifikt it-system og privathed. Tilgangen er også ofte reaktiv, hvilket kan være problematisk, da privathed ikke er en værdi, der nemt kan tilføjes, efter en teknologi er taget i anvendelse.

Jeg opfatter i afhandlingen VSD og PbD som to mulige tilgange til at realisere værdier i teknologi. Formålet med disse tilgange er at løse it-etiske problemstillinger, hvilket er illustreret i nedenstående figur 1.



Figur 1: It-etik og værdibaseret design

Anvendelsen af VSD og PbD til at løse it-etiske problemstillinger kan være fordelagtig, idet disse tilgange netop tager hensyn til, at flere værdier er i spil på samme tid i en teknologi.

Jeg vil nu vende tilbage til Moors definition af it-etik. Denne definition kan bruges til at illustrere, at afhandlingen netop er et it-etisk projekt. It-etik omfatter ifølge Moor blandt andet analyse af en teknologis beskaffenhed og samfundsmæssige betydning (Moor J. H., 1985, s. 266). *Dataveillance* og den indflydelse, brugen af *dataveillance* har på samfund og individ, diskuteres i kapi-

tel 3., *Overvågning og implikationer heraf*. Ydermere diskuteres sikkerhedsteknologier i kapitel 7., *Dataveillance af big data som sikkerhedsteknologi*.

It-etik handler ifølge Moor også om at formulere og begrunde politikker for etisk brug af informationsteknologi. I kapitel 4., *Informationel privathed,* argumenteres for, at informationel privathed er en værdi for såvel stat som samfund og individ. Hermed kan det begrundes, at politikkerne for, hvordan informationel privathed og offentlig sikkerhed implementeres i teknologi, bør tilgodese stat, samfund og individ.

VSD og PbD kan i lyset af Moors definition opfattes som et potentielt middel til at udforme etisk forsvarlig teknologi og til at understøtte eller vanskeliggøre bestemt teknologianvendelse. Præmissen herfor er en forståelse af, at udviklingen af en given teknologi ikke determinerer brugen, når teknologien tages anvendelse, men at udviklingsfasen stadig har betydning for slutproduktet. De beslutninger, der tages i forbindelse med udvikling af teknologi, har indflydelse på, hvilke brugsmuligheder en given teknologi har. Der er således i et vist omfang mulighed for at påvirke brugen i en ønskværdig retning.

2.2. AFHANDLINGEN I LYSET AF ANDEN FORSKNING OG AFGRÆNSNING

I nedenstående findes indledningsvis en diskussion af afhandlingens tværfaglige tilgang til den problemstilling, jeg behandler. Dernæst præciseres det, hvorved afhandlingen adskiller sig fra anden forskning. Hermed bliver det også eksplicit, hvori det selvstændige bidrag i projektet består.

Nærværende ph.d.-afhandling er tværfaglig og behandler således problemfelter ved at trække på viden fra en række fagområder – eksempelvis sociologi, filosofi, jura, datalogi, politologi og kriminologi. At behandle en problemstilling tværfagligt betyder også, at afhandlingen er horisontal i sin tilgang til problemstillinger. Der er således tale om, at problemområder behandles bredt og favnende. I forhold til den konkrete problemstilling, som behandles her, vurderer jeg, at tværfagligheden og projektets bredde er en styrke. Det er i

kraft den tværfaglige og horisontale tilgang til problematikker, at projektet adskiller sig fra anden forskning.

Tværfagligheden betyder, at de enkelte fagområder isoleret set vil blive behandlet mere overordnet, end man ville gøre, hvis man udelukkende behandlede en problemstilling med udgangspunkt i isolerede fagligheder. Havde en mere vertikal tilgang til dele af den problemstilling, som behandles her, været anlagt, ville det have været muligt at behandle dele af projektet mere detaljeret. Omvendt havde en sådan vertikal tilgang været på bekostning af den samlede behandling af en problemstilling forankret i en kompleks praksis. Afhandlingens tværfaglighed indebærer således et "brobyggerperspektiv" mellem forskellige fagligheder. Dette brobyggerperspektiv er netop også, hvad jeg i kraft af min informationsvidenskabelige baggrund kan tilbyde. I afhandlingen er jeg også handleanvisende, idet jeg vurderer, hvorvidt VSD og PbD er anvendelige i forbindelse med udvikling af sikkerhedsteknologi. En kvalificeret diskussion, der behandler brugen af disse tilgange i udviklingen af sikkerhedsteknologi, forudsætter en tværfaglig tilgang. Designtilgangene rummer spørgsmål af dyb, filosofisk karakter, hvilket dog skal ses i lyset af en praksis præget af teknologi. Jeg mener, at den måde, jeg tilgår problemet her, er velbegrundet, idet tilgangen er betingelsen for at kunne give samlet overblik over området.

Formålet med dette forskningsprojekt er at behandle en problemstilling, der kun synes at tage til i omfang – nemlig staters *dataveillance* af individers data. Ydermere er det formålet med afhandlingen at være handleanvisende i forhold til, hvorvidt VSD og PbD kan finde anvendelse i sikkerhedsteknologi. Afhandlingen placeres kontekstuelt i sin samtid, hvilket sker i kraft af de nutidige eksempler på overvågning, der inddrages. Samtidigt hermed mener jeg, at problemstillingen i afhandlingen belyses på en måde, så vurderingerne og udsagnene får en generel karakter.

Informationel privathed, offentlig sikkerhed og spændingen herimellem er ikke kun en problematik, der knytter sig til en specifik sikkerhedsteknologi. Det er snarere en grundlæggende problemstilling, der er forbundet med alle

sikkerhedsteknologier, der bruges til at overvåge data. Ønsket om, at afhandlingens vurderinger skal have en større rækkevidde end blot til nogle konkrete teknologier, reflekteres også i valget af sikkerhedsteknologier. De sikkerhedsteknologier, der inddrages, optræder som scenarier i afhandlingen og udgør et diskussionsgrundlag med henblik på at illustrere teoretiske pointer. Sikkerhedsteknologierne har det fællestræk, at de alle er udviklet med henblik på at overvåge data – det vil sige *dataveillance*. De data, der anvendes som ressource for *dataveillance,* kan endvidere karakteriseres som *big data*.

Sikkerhedsteknologierne er dog også valgt under hensyntagen til de forskelligheder, der er imellem dem. Sikkerhedsteknologier sigter imod to forskellige typer af kriminalitet, nemlig terror og organiseret kriminalitet. Desuden opererer de med forskelligt sigte - strategisk, taktisk eller operationelt. Slutteligt er der forskel på, hvilke statslige organer der sandsynligvis vil gøre brug af sikkerhedsteknologier. Jeg uddyber begrundelsen for sikkerhedsteknologierne i forbindelse med, at disse præsenteres i kapitel 7., *Dataveillance af big data som sikkerhedsteknologi.*

Afhandlingens tværfaglighed er med til at adskille projektet fra anden forskning, der på forskellig vis grænser op til afhandlingen.

I afhandlingen tager jeg primært udgangspunkt i en kontekstuel forståelse af privathed i forhold til information (Moor J. H., 1997; Nissenbaum, 2010). Derudover argumenterer jeg for, at privathed er et fælles gode (Gavison, 1984; Regan, 2002; Regan, 1995). Denne opfattelse af privathed medfører, at det er relevant at forandre forholdet mellem offentlig sikkerhed og informationel privathed i sikkerhedsteknologi. Afhandlingen udfordrer således synet på spændingen mellem offentlig sikkerhed og privathed.

Det behandles til slut i afhandlingen, om udvalgte værdibaserede designtilgange er anvendelige til at realisere informationel privathed og offentlig sikkerhed i sikkerhedsteknologi. VSD er blevet diskuteret, og anvendeligheden heraf er demonstreret i forhold til et bredt udsnit af teknologier. Blandt disse kan nævnes UrbanSim, der er software til at modellere og simulere byplanlægning og miljøpåvirkning (Friedman, Kahn, & Borning, 2006, s. 357-358),

cookies med informeret samtykke i en webbrowser (Friedman, Kahn, & Borning, 2006, s. 352-353; Friedman, Lin, & Miller, 2005), privathed i en webbrowser (Xu, Crossler, & Bélanger, 2012), The augmented window, der er en plasmaskærm på et kontor uden vindue, der viser, hvad der foregår udenfor (Friedman, Kahn, & Borning, 2006, s. 353-357), nanofarmaci (Timmermans, Zhao, & van den Hoven, 2011), vindmøller og vindmølleparker (Oosterlaken, 2015), sensorteknologi (Dechesne, Warnier, & van den Hoven, 2013) og krigsmissiler (Cummings, 2006). Timmermans og Mittelstadt har diskuteret refleksivitet (eller mangel på samme) i forhold til VSD, hvilket er begrundet med og løst koblet til afsløringerne af NSA's overvågning i sommeren 2013 (Timmermans & Mittelstadt, 2014).

PbD er centreret om privathed i systemudvikling og har været sat i forbindelse med blandt andet emner som datamining (Monreale, 2011), big data (Cavoukian, Stewart, & Dewitt, 2014), datasikkerhed (Cavoukian & Chanliau, 2013), biometri og offentlig sikkerhed (Cavoukian, 2012a).[47] I nærværende afhandlingen vil jeg belyse PbD's anvendelighed fra et pragmatisk perspektiv.

Med afhandlingen udfoldes perspektivet på VSD og PbD i forhold til sikkerhedsteknologier med afsæt i en forståelse af privathed som en kontekstuel størrelse. Derudover betones det, at diskussionen af sikkerhedsteknologier i forhold til VSD og PbD er pragmatisk, idet det herved kan vurderes, om VSD og PbD er anvendelige med henblik på at nedsætte spændingen mellem informationel privathed og offentlig sikkerhed. Således bliver VSD diskuteret og vurderet i forhold til sikkerhedsteknologi.

Jeg er ikke den første, der har haft berøring med hele eller dele af den problemstilling, som diskuteres i afhandlingen. Eksempelvis har van Leonen et al (2007) og Aquilina (2010) begge behandlet værdierne privathed og sikkerhed i artikler, hvor vurderingerne dog primært er juridiske. Både Regan (1995) og Gavison (1984) har argumenteret for, at privathed er et fælles gode – i afhandlingen bringes disse argumenter i spil i forbindelse med overvågning af indivi-

[47] PbD har også været anvendt på en række andre områder. Se reference for oversigt (Cavoukian, 2012b, s. 56-59)

ders data. Monreale (2011) har beskæftiget sig med datamining og PbD i sin ph.d.-afhandling, men denne er et væsentligt mere teknisk bidrag end nærværende ph.d-afhandling. Thuraisingham (2002) har behandlet datamining inden for rammen af national sikkerhed, privathed og civile rettigheder, hvor der er et smallere fokus på en konkret udfordring i datamining - et inferensproblem. Tavani (1999) har diskuteret *knowlegde discovery* og datamining i lyset af privathed, hvilket dog ikke handler om statslige organers indsamling af individers data. Gürses (2010) har behandlet privathed, men dog i relation til *sociale netværksservices*. Van Lieshout et al (2013) plæderer for, at privathed og sikkerhed ikke skal behandles med henblik på en afvejning af de to værdier i forhold til hinanden. Man skal derimod forsøge at forene værdierne. Hiranandani (2011) har ligeledes udfordret ideen om, at privathed og sikkerhed bør afvejes indbyrdes. Begge artikler beskæftiger sig med samme problemstilling, som behandles i aktuelle afhandling, og har derfor kunnet bidrage med interessante perspektiver og inspiration.

Som det nu er tydeligt, trækker afhandlingen på viden fra en række særdeles forskellige fagområder. Afhandlingens styrke og originalitet består i at udgøre et samlet argument for og en tværfaglig vurdering af, hvordan det er hensigtsmæssigt at anskue staters overvågning af individer med henblik på at opretholde offentlig sikkerhed.

Afhandlingen bidrager til den akademiske litteratur, idet kendte perspektiver her forenes på en ny måde. Idet en aktuel og samfundsrelevant problemstilling, der ofte diskuteres i den offentlige debat, her er under behandling, kan afhandlingens argumenter og konklusioner også bruges til at bringe et nyt perspektiv ind i debatten om, i hvilken grad stater bør overvåge individers data.

2.2.1. AFGRÆNSNING OG FRAVALG

I forbindelse med introduktionen til de enkelte kapitler begrundes det, med hvilket afsæt og ud fra hvilken vinkel de enkelte kapitler i afhandlingen er behandlet. Det skal bemærkes, at jeg behandler spændingen mellem offentlig sikkerhed og privathed i sikkerhedsteknologier i demokratiske stater.

Slutteligt er det også værd at bemærke, at denne afhandling ikke beskæftiger sig med it-sikkerhed. It-stikkerhed og sikker opbevaring af data er nært beslægtet med indsamling af data og dermed også med privathed. Det er klart, at en utilstrækkelig it-sikkerhed kan medføre kompromittering af individers privathed. Det er dog ikke formålet med afhandlingen at behandle dette område.

2.3. KONVENTIONER I AFHANDLING

Nedenfor præciseres en række konventioner anvendt i afhandlingen. Disse konventioner omhandler oversættelser, kurvisering og lignende. Indledningsvist findes en begrebsafklaring.

Begrebsafklaringer

Det er relevant at afgrænse en række begreber i afhandlingen. Disse begreber vil blive præciseret og diskuteret senere.

- **Stat** henviser i afhandlingen til en politisk konstruktion, der hviler på en politisk, filosofisk forståelse af, at mennesker går sammen for at sikre sig selv. I afhandlingen anses staten for at være mere end blot summen af individer. Denne antagelse ligger implicit i afhandlingens problemstilling, idet den er forudsætningen for, at problemstillingen overhovedet har relevans. Er staten ikke mere end blot summen af individer, vil staten ikke kunne sætte individets privathed under pres.
- **Statsligt organ** henviser til et konkret organ, der tilhører staten. Der kan for eksempel være tale om en efterretningstjeneste eller politi.
- **Samfund** er en gruppering. Eksempelvis kan nævnes et lokalsamfund, det danske samfund eller det vestlige samfund. Begrebet intern sikkerhed referer til samfundets sikkerhed.
- **Borger** er et individ i en stat.
- **Medlemsland** henviser til et land, der er medlem af Den Europæiske Union.
- **Value Sensitive Design** (VSD) betegner en konkret tilgang og metodologi, som er udviklet af Batya Friedman med flere (Friedman, Kahn,

& Borning, 2006). Betegnelsen Value Sensitive Design har siden starten af 1990-erne bevæget sig fra at være et paraply-begreb, hvor det fælles fundament var fokusering på menneskelige værdier i teknologi, til i dag, hvor Value Sensitive Design i følge Davis og Nathan (2015) er en term, der udpeger en mere specifik strategi og en række teknikker til konkret anvendelse i design (Davis & Nathan, 2015, s. 11-12).

- **Privacy by Design** (PbD) betegner et konkret værktøj til at realisere privathed i design. PbD er udviklet i 1990'erne af den canadiske Information & Privacy Commissioner, Ann Cavoukian (Cavoukian, 2011).
- **Værdibaseret design** er en fællesbetegnelse, der omfatter Value Sensitive Design, Privacy by Design og i nogle tilfælde også Values At Play.

Om oversættelser anvendt i afhandlingen

Såfremt jeg selv har oversat et ord eller et begreb, er det oprindelige ord eller begreb anført i fodnote, første gang det optræder. Det oversatte ord eller begreb i fortløbende tekst er kursiveret første gang, det optræder.

- I afhandlingen har jeg anvendt den engelske oversættelse "Discipline and Punish: The Birth of the Prison" (Foucault, 1995) af Michel Foucaults "Surveiller et punir: Naissance de la Prison". For læsevenlighedens skyld har jeg dog valgt at bruge den danske oversættelse af centrale begreber i Foucaults værk. Jeg har benyttet en oversættelse af Mogens Chrom Jacobsen (Foucault, 2002). Første gang en sådan oversættelse fra engelsk til dansk optræder, er der gjort opmærksom herpå i en fodnote, hvor det engelske begreb er anført.
- I afhandlingen er Thomas Hobbes "Leviathan" anvendt på originalsproget engelsk (Hobbes, 2001). I nogle få tilfælde er der benyttet oversættelser til dansk af begreber fra Leviathan. Jeg har anvendt en oversættelse af Claus Bratt Østergaard (Hobbes, 2008).
- I afhandlingen har jeg brugt en engelsk oversættelse af Immanuel Kants "Grundlegung zur Metaphysik der Sitten" (Kant, 1781). Jeg har anvendt en oversættelse af Allen W. Wood (Kant, 2002).

Såfremt jeg ikke har fundet det hensigtsmæssigt at oversætte et ord eller begreb, er dette kursiveret, hver gang det optræder i fortløbende tekst. Der er gjort opmærksom herpå i en note, første gang det optræder.

Litteratur fra antologier og genudgivelser

Jeg har anvendt artikler, der er trykt i en antologi, og bøger, som tidligere har været publiceret andetsteds. Det betyder, at det årstal, der er anført i referencen i fortløbende tekst, ikke afspejler det tidspunkt, hvor den enkelte artikel eller bog er skrevet og udgivet. Første gang en sådan reference optræder, vil det være anført i en fodnote, hvornår artiklen eller bogen blev publiceret første gang.

2.4. KAPITELPRÆSENTATIONER

For læsevenlighedens skyld findes der i nedenstående en kort introduktion til de enkelte kapitler.

Kapitel 3., *Overvågning og implikationer heraf*

Kapitel 3 består af to dele og omhandler overvågning og dennes implikationer. Det er relevant at behandle overvågning, idet overvågning anvendes som et middel til at opretholde offentlig sikkerhed.

Kapitlets første del, *Overvågning i samfundet,* belyser overvågning med afsæt i en sociologisk forståelse. Det sociologiske perspektiv på overvågning er særligt tydeligt, idet overvågning opfattes som en konsekvens af bureaukratiet og ikke som et ønske om et totalitært "big brother"-samfund. En række definitioner på overvågning diskuteres og sammenlignes, ligesom magtbalancen mellem overvåger og overvågede ved forskellige typer af overvågning behandles.

Kapitlets anden del, *Overvågning: Implikationer for stat, samfund og individ,* behandler overvågningens implikationer, hvilket diskuteres på såvel sociologiske som filosofiske præmisser. Konsekvenserne af overvågning diskuteres med afsæt i en række temaer, der kan opfattes som en katalogisering af nogle af de risici, der kan være forbundet med overvågning. Her behandles social kontrol, overvågningens betydning for intellektuel privathed samt overvåg-

ningens påvirkning af menneskets autonomi og anonymitet. Slutteligt diskuteres overvågning i forhold til social sortering, idet sidstnævnte indenfor afhandlingens kontekst kan anvendes til at udpege personer eller grupper, der menes at udgøre en risiko i forhold til offentlig sikkerhed.

Kapitel 4., *Privathed*

Kapitel 4 består af fire dele og omhandler privathed som en værdi for individet og som et fælles gode. Det er relevant at belyse privathed, da privathed kan komme under pres, når stater overvåger individers data. Privathed behandles i kapitlet med et filosofisk afsæt.

Kapitlets første del, *Privathedens semantik,* belyser meningen med begreberne privat og privatliv. Der inddrages en række begrebsforklaringer fra ordbøger, hvilket illustrerer en forståelse af privathed, der tager afsæt i en sondring mellem offentlig og privat. Samtidigt demonstreres det, at privathed er vanskeligt at definere, og der rejses en diskussion af de begrebsforklaringer, der er inddraget.

Kapitlets anden del, *Perspektiver på informationel privathed,* belyser en række centrale perspektiver på privathed. Afsnittet falder i to underafsnit, hvoraf det første, *Privathed som kontrol versus begrænset adgang,* belyser og diskuterer en række fremtrædende tilgange til privathed. Desuden inddrages i denne diskussion også privathed i forhold til sociale relationer og intimitet.

Det andet underafsnit, *Kontekstuel forankret informationel privathed,* diskuterer privathed forstået med afsæt i en kontekstuel forankring. Her er den grundlæggende antagelse, at det ikke er meningsfuldt at hævde, at information er privat *per se*, og ej heller at diskutere, om information er offentlig eller privat. Derimod er det afgørende, om en given information er passende i en given kontekst, og om informationer bevæger sig på passende vis.

Kapitlets tredje del, *Privathed som et fælles gode,* diskuterer privathed forstået som et instrumentelt gode, der ikke kun er væsentligt for det enkelte individ, men også for staten og samfundet. Privathed knyttes eksempelvis til en værdi som demokrati.

Kapitels fjerde del, *Privathed – "intet at skjule"-argumentet,* behandler det synspunkt, at hvis man intet har at skjule for den overvågende stat, så har man intet at frygte i forhold til statens overvågning. Dette argument optræder ofte i forskellige udgaver i forbindelse med balancering af sikkerhed og privathed og er derfor relevant at diskutere.

Kapitel 5., ***Databeskyttelse: Retskilder og etikkens berettigelse***

Kapitel 5 består af 2 dele og omhandler dels retskilder med relevans for databeskyttelse, dels etiske overvejelsers berettigelse i lyset af den juridiske regulering af databeskyttelse. Det er relevant at behandle retskilder, der omhandler databeskyttelse, da disse retskilder sætter begrænsninger for, hvordan personhenførbare data må anvendes. I lyset af disse retskilder demonstreres det, hvorfor spændingen mellem privathed og sikkerhed er relevant at behandle i et etisk perspektiv.

Kapitlets første del, *Retskilder vedrørende databeskyttelse i den Europæiske Union,* behandler en række af retskilder, der angår databeskyttelseslovgivning i EU. Denne lovgivning er på nuværende tidspunkt reguleret med det europæiske databeskyttelsesdirektiv, 95/46/EF. Ydermere berøres den historiske udvikling, som de retskilder, der har relevans for databeskyttelse, har undergået. Til slut i den første del af kapitlet belyses også en række amerikanske retskilder, der hviler på et utilitaristisk grundlag. Hermed demonstreres det, at der er markant forskel i den måde, EU tilgår databeskyttelse, og måden, hvorpå USA varetager privathedsbeskyttelse.

I kapitlets anden del, *Etikkens berettigelse og ansvarlig udvikling af teknologi,* argumenteres der for, at etiske overvejelser er berettigede, selvom databeskyttelse er reguleret af retskilder. Denne argumentation falder i tre dele. For det første argumenteres der for, at etik kan anses for at være juraens fundament. Etik går således forud for jura. For det andet gøres der gældende, at etik kan supplere retskilder. Denne betragtning hviler på det forhold, at selv lovlige aktiviteter kan give anledning til overvejelser om etisk forsvarlighed. For det tredje påpeges det, at databeskyttelsesdirektivet og de værdibaserede design-tilgange, som behandles i afhandlingen, udøver databeskyttelse på

forskellige måder. Databeskyttelsesdirektivet i EU har registerfører og registeransvarlig i centrum. Værdibaserede design-tilgange påpeger derimod vigtigheden af at tænke databeskyttelse ind i designet allerede fra det øjeblik, udviklingen af en teknologi påbegyndes. Slutteligt introduceres og diskuteres såkaldt *responsible research and innovation*, der er et fokusområde i EU.

Kapitel 6., *Offentlig sikkerhed*

Kapitel 6 omfatter to dele, og emnet er offentlig sikkerhed. Det er relevant at behandle offentlig sikkerhed, idet offentlig sikkerhed netop er en af de værdier, der behandles i afhandlingen. Offentlig sikkerhed vægtes ofte højere end informationel privathed. Styrkelse af den offentlige sikkerhed kan således give anledning til bekymring for, at informationel privathed.

I kapitlets første del, *Offentlig sikkerhed og relationen mellem stat og individ,* tages der afsæt i social kontraktteori med henblik på at diskutere det ontologiske forhold mellem stat og individ. Diskussionens udgangspunkt er motivationen for, at stat og borger indgår i en relation. Forskellige perspektiver på forholdet mellem stat og individ inddrages, og der argumenteres for, at et liberalistisk synspunkt, hvor det frie individ er i centrum, er hensigtsmæssigt. Det følger af afhandlingens genstandsfelt, at staten er mere end blot summen af individer. Var det ikke tilfældet, ville det ikke være muligt for staten at sætte individets privathed under pres. Der kastes desuden et historisk blik på udviklingen i opfattelsen af sikkerhedsbegrebet. Sikkerhed er ikke længere opfattet som en størrelse, der knytter sig til staten alene, men også til individet.

Kapitlets anden del, *Sikkerhedsbegrebet i udvalgte retskilder,* belyser en række retskilder med relevans for sikkerhed. Det eksemplificeres her, hvordan sikkerhed kan være et middel til at begrænse en rettighed som privathed jævnfør menneskerettighedskonventionens art. 8. Sikkerhed præsenteres endvidere som en negativ individuel ret, hvormed det udpeges, at staten skal undlade at kompromittere individets fundamentale rettigheder. Det diskuteres ligeledes, hvordan sikkerhed kan opfattes som statens positive forpligtigelse til at påse, at individet er i en tilstand af sikkerhed.

Kapitel 7., *Dataveillance* af *big data* som sikkerhedsteknologi

Kapitel 7 består af to dele og behandler overvågning af *big data* anvendt i sikkerhedsteknologier.

I kapitlets første del præciseres det, hvad *big data* er. Det interessante ved *big data* er ikke kvantiteten af data, men derimod de muligheder der er for dataanalyse. *Big data* diskuteres i lyset af randomiserede stikprøver og repræsentative data. Desuden problematiseres *big data* i forhold til, at ikke alle individer bidrager til *big data*, hvilker betyder, at nogle bliver ekskluderet fra de beslutninger, der bliver taget på grundlag af data. Ydermere behandles *big data* i lyset af begreberne kausalitet og korrelation. Slutteligt gives der eksempler på visualisering af *big data,* hvilket kan være en betydelig hjælp til at forstå *big data.*

I kapitlets anden del, *Big data som ressource for intelligence-led policing,* præsenteres indledningsvis *intelligence-led policing,* der er en ledelsesfilosofi. Efterfølgende introduceres tre typer af sikkerhedsteknologier. Formålet her er at illustrere, hvordan politi og efterretningstjenester kan anvende *big data* med henblik på at opretholde sikkerhed. Disse teknologiers præsentation udgør tillige et diskussionsgrundlag med henblik på at kunne fremsætte teoretiske pointer. De tre sikkerhedsteknologier sigter mod enten organiseret kriminalitet eller terror.

Predictive policing, der er et strategisk og operationelt værktøj, anvendes af politiet til på baggrund af statistisk analyse at forudsige øget risiko for kriminalitet. *Environmental scanning*, der primært anvendes strategisk, bruges til at scanne det eksterne miljø for information med henblik på at kunne forudsige trends og påvise tidlige, svage tegn på kriminalitet. Som i eksemplet anvendt i afhandlingen kan environmental scanning dog også få et operationelt formål. Slutteligt inddrages en teknologi til terrornetværksanalyse. Det er et videnhåndteringssystem, der kan støtte personer i at modellere et terrornetværk, hvilket er yderst komplekst.

Kapitel 8., *Realisering af værdier i design*

Kapitel 8 består af tre dele og berører to udvalgte designtilgange til at realisere værdier i design. Det er relevant at vurdere, om VSD og PbD har potentiale til at realisere værdier i sikkerhedsteknologi. Såvel VSD som PbD behandles i en pragmatisk ramme, og det er også med dette udgangspunkt, at der foretages en vurdering af disse metoders anvendelighed.

I kapitlets første del, *Value Sensitive Design,* præsenteres og diskuteres VSD med henblik på at vurdere, om denne tilgang er anvendelig til at realisere værdier i sikkerhedsteknologi. VSD er en tredelt, iterativ metodologi til proaktivt at realisere værdier i teknologi. En række problemstillinger i forhold til VSD udpeges og diskuteres – eksempelvis hvorvidt der findes universelle værdier, om VSD's manglende normative ståsted er en hæmsko, og hvilken rolle en designer har i et projekt.

I kapitlets anden del, *Privacy by Design,* præsenteres og diskuteres PbD, der specifikt har fokus på privathed og består af syv grundlæggende principper. Det undersøges ydermere, om PbD-principperne er anvendelige i praksis.

I kapitlets tredje del, *Vurdering: Værdibaseret design og sikkerhedsteknologi,* konkluderer jeg, at disse tilgange skønnes anvendelige, til trods for at begge tilgange har en række udfordringer. Der argumenteres for, at en af de måder, hvorpå man kan imødekomme flere af de problemstillinger, som knytter sig til VSD og PbD, er at sikre en bred faglighed i forbindelse med udvikling af ny teknologi.

Kapitel 9., *Konklusion*

Kapitel 9 udgør afhandlingens konklusion. Her findes en kort opsamling på afhandlingens hovedpointer.

3. OVERVÅGNING OG IMPLIKATIONER HERAF

3. OVERVÅGNING OG IMPLIKATIONER HERAF

Anvendelse af sikkerhedsteknologier leder ofte til mere overvågning (PRISE, s. 1). Det skal bemærkes, at der er undtagelser, idet ikke alle sikkerhedsteknologier nødvendigvis involverer overvågning. På sammen måde er målet med alle overvågningsteknologier ikke nødvendigvis sikkerhed. Det lader dog til at være rimeligt at hævde, at: "[...] the classic configuration sees surveillance presented as a means with security as an end." (European Commission, 2014a, s. 24). Af denne grund må det være relevant at undersøge overvågning nærmere, herunder hvad dette begreb inkluderer og implikationerne af overvågning for stater og individer.

Overvågning er et komplekst, interdisciplinært genstandsfelt. Overvågningens kompleksitet er blevet øget som følge af blandt andet teknologiens muligheder. I dag taler man ikke bare om "overvågning", men om eksempelvis "social surveillance", "sousveillance", "participatory surveillance", "counterveillance", "uberveillance" og "shadow surveillance". At det har været nødvendigt at øge mængden af begreber til at beskrive overvågning, vidner om den øgede kompleksitet. Denne kompleksitet kan også demonstreres med en af Anders Albrechtslund (2008) udformet liste, der indeholder 23 forskellige perspektiver på overvågning (2008, s. 50-52).

Indenfor den engelsk-amerikanske forskningstradition er overvågning ofte undersøgt fra en sociologisk vinkel. De humanistiske, sociale og tekniske fagområder har dog også interesseret sig for området som følge af overvågningens relation til blandt andet politologi, kriminologi, datalogi og jura (Albrechtslund, 2008, s. 37).

De kilder, der har dannet grundlag for nærværende kapitel, hvor en teoretisk udredning, indkredsning og diskussion af begrebet overvågning findes, er primært af sociologisk karakter (Gandy, 1996; Lyon, 2007; Marx, 2002; Rule, 1973). Det vil med andre ord sige, at overvågning beskrives som et fænomen i samfundet, og der redegøres for den funktion, overvågning har i samfundet.

Albrechtslund (2008) har defineret det sociologiske perspektiv på overvågning som: "Modern society is by definition a surveillance society, because monitoring practices are an important building block to protect rights, maintain law and order collect taxes, etc." (Albrechtslund, 2008, s. 51). James Rule (1973), der var den første til at give en sociologisk redegørelse for dagligdagsovervågning (Lyon, 2007, s. 80) med bogen "Private Lives and Public Surveillance" (Rule, 1973), argumenterer heri for, at de spørgsmål, der omhandler den øgede masseovervågning i dag, helt grundlæggende er sociologiske, idet:

> "[...] the compelling concerns on this topic are not just over the possible effects of this or that surveillance technique as such, but over the broad social trends which shape the customary uses of such techniques." (Rule, 1973, s. 34).

Rule behandler overvågningens rolle i det moderne samfund, hvilket også er den synsvinkel overvågning vil blive belyst med i denne afhandlingen. I kraft af at afhandlingen beskæftiger sig med den postmoderne, teknologisk medierede overvågning, spiller teknologi i forhold til overvågning ligeledes en betydningsfuld rolle.

Det er ifølge Lyon muligt at udpege tre forskellige, "konstruerede" tidsperioder i udviklingen af overvågning. Disse perioder skal ikke opfattes som størrelser, der afløser hinanden, men mere som et værktøj til forståelse af udviklingen (Lyon, 2007, s. 74-75). Den før-moderne overvågning i antikken blev realiseret face-to-face eller som en mere traditionel form for aflytning end den, man er vidne til i dag. Den moderne overvågning etableredes primært som følge af bureaukratiet, der på baggrund af den viden, som var tilgængelig om individet, havde en vis magt. Dette er ligeledes demonstreret i Panoptikon og er et centralt emne i Foucaults analyser heraf (Foucault, 1995, s. 200; Lyon, 2007, s. 80-81). Den bureaukratiske overvågning er ligeledes nært forbundet med Foucaults ide om den tætte forbindelse mellem magt og viden: Viden giver magt til at kontrollere individer, og magt giver viden (Foucault, 1995). Mere praktisk kommer dette eksempelvis til udtryk som klassifikation af individer, der spiller en særlig rolle i forhold til retshåndhævelse op igennem det attende og nittende århundrede, hvor en bevægelse mod mere regulering og organisering forekommer (Lyon, 2007, s. 79-85). Den postmoderne overvåg-

ning har Gary Marx (2002) blandt andet forsøgt at indfange med begrebet new surveillance, der beskriver en række særlige kendetegn ved overvågning i dag. Eksempelvis kan nævnes, at denne overvågning er billig, mindre synlig og typisk sker på afstand i en automatiseret proces, der kan foretage intensiv overvågning i realtid (Marx, 2002, s. 28-29)

Afhandlingens sociologisk inspirerede belysning af overvågning indebærer et syn, hvor staten som strukturel entitet er den overvågende part, og hvor overvågningen er vævet ind i hele det statslige apparat. Idet afhandlingen netop undersøger en problemstilling, hvor staten er den overvågende part, synes denne tilgang at være hensigtsmæssig. Det sociologiske perspektiv i afhandlingen betyder også, at den senere brug af begrebet "overvågningssamfund" ikke skal opfattes som en "paranoid" tilgang, hvor overvågning opfattes som et skjult komplot mellem staten og organisationer (Albrechtslund, 2008, s. 51). Opfattelsen i afhandlingen er i stedet, at den udbredte overvågning i dag kan forklares af bureaukratiets udvikling, hvilket netop er det sociologiske perspektiv (Albrechtslund, 2008, s. 51). Det betyder imidlertid ikke, at overvågning er uproblematisk, eller at man bør igangsætte og udføre overvågning efter forgodtbefindende.

For overskuelighedens skyld er nærværende kapitel struktureret omkring en række temaer, der er relevante for overvågning. Det er ikke formålet at give en udtømmende behandling af overvågning i bredeste forstand. Derimod er hensigten at komme en forståelse af begrebet overvågning nærmere og "zoome" ind på temaer, der er relevante for den kontekst, afhandlingen befinder sig i – overvågning som middel til at opnå offentlig sikkerhed.

I afsnit 3.1., *Overvågning i samfundet,* diskuteres overvågning og dennes rolle i samfundet. Jeg belyser her en række relevante temaer i forhold til afhandlingen. Eksempelvis omtales den magtrelation, der eksisterer mellem overvåger og overvågede. Ydermere belyses forskellen mellem traditionel overvågning og såkaldt *new surveillance*. I afsnit 3.2., *Overvågning: Implikationer for stat, samfund og individ* belyses og diskuteres en række implikationer af overvågning i relation til afhandlingens genstandsfelt.

3.1. OVERVÅGNING I SAMFUNDET

Verbet at overvåge betyder ifølge Den Danske Ordbog blot det "at holde øje med, for eksempel for at beskytte eller kontrollere" (ordnet.dk, overvåge). Det engelske ord for overvågning, *surveillance*, har etymologisk set rødder i det franske "sur" og "veiller", der betyder henholdsvis "over" (ordbogen.com, sur) og "våge" (ordbogen.com, veiller). Betydningen af at overvåge indebærer, at nogen våger over nogen eller noget.

Overvågning i bred forstand kan siges at have eksisteret altid i kraft af menneskers interpersonelle relationer (Ball, Lyon, Wood, Norris, & Raab, 2006, s. 1; Lyon, 2007, s. 74). Eksempelvis kan der her være tale om noget så simpelt som forældres overvågning af deres børn, når de leger i haven. Nogle vil formentlig argumentere for, at dette ikke er "rigtig overvågning", men et fænomen der derimod skal forklares med afsæt i prædikater som "beskyttelse", "omtanke" og "omsorg". Lyon diskuterer denne problematik, hvorom han gør klart, at overvågning ikke er enten omsorg eller kontrol, men at der er tale om et kontinuum mellem disse to poler (Lyon, 2007, s. 14). Ofte vil der således være tale om, at overvågning indeholder elementer af begge. Eksemplet illustrerer samtidigt, at overvågning i bredeste forstand kan karakteriseres som en grundlæggende del af vores dagligdags liv, hvilket omvendt betyder, at det kan være svært præcist at udpege og afgrænse, hvad overvågning egentlig er (Lyon, 2003, s. 164). Forskellige definitioner på overvågning og en diskussion heraf vender jeg tilbage til i 3.1.1., *Fra traditionel overvågning til new surveillance*.

Vi lægger i dag i mindre og mindre grad mærke til overvågning, som en følge af at overvågning er blevet en naturligt indlejret del af vores daglige liv og findes alle vegne. Interessant er det også, bemærker Lyon, at individer i dag indvilger i overvågningen, idet de er blevet vant til denne overvågning (Lyon, 2014, s. 72). Så godt som alle rige og velstående lande kan nu til dags rubriceres som såkaldte *overvågningssamfund,* idet indsamling og behandling af data er allestedsforekommende (Ball, Lyon, Wood, Norris, & Raab, 2006, s. 1; Stalder, 2002, s. 120). En ofte anvendt metafor for overvågningssamfundet såvel i

den offentlige debat som i den akademiske verden er *Big Brother*. Denne metafor stammer fra John Orwells roman "1984" (Orwell, 1949) om det totalitære og teknisk avancerede samfund, Oceania. Historien udspiller sig i London, hvor "big brother is watching you". Big Brother er den allestedsnærværende myndighed, der kan høre og se alt døgnets fireogtyve timer. (Orwell, 1949).

Rækkevidden og diversiteten af overvågning har ligeledes forandret sig, og de forskellige typer af overvågning, vi i dag har til rådighed, er uden fortilfælde i historien (Richards, 2013, s. 1936). I kraft af teknologi har overvågning udviklet sig til ikke kun at være et lokalt fænomen, men også en global størrelse der ydermere kan beskrives med prædikater som "allestedsnærværende", "konstant" og "uundgåelig". Det betyder i praksis, at overvågning ikke længere behøver foregå fysisk i nærheden af den eller det, man ønsker at overvåge (Lyon, 2007, s. 25; Lyon, 2003, s. 1; Marx, 2002, s. 28-29). Hvor det tidligere var et menneske, der foretog overvågning, er overvågning af data i dag typisk en delvist eller fuldt ud automatiseret proces foretaget af en maskine. Overvågning i dag er ydermere kendetegnet ved at være langt mere kosteffektiv end den "traditionelle overvågning". "Traditionel overvågning" henviser her til ikke teknologisk medieret overvågning. Begrebet skal ses i lyset af Gary Marx' betegnelse new surveillance, som vil blive præsenteret senere (Marx, 2002).

Overvågningssamfundet bygger på en grundlæggende antagelse om, at indsamling af data er en væsentlig effektivitetsfremmende foranstaltning. Ifølge Lyon bør overvågningssamfundet opfattes som et produkt af moderne organisations- og regeringsformer, der i høj grad har oprindelse i det bureaukrati, der vandt særligt indpas i forbindelse med industrialiseringen (Ball, Lyon, Wood, Norris, & Raab, 2006, s. 1; Lyon, 2007, s. 79). At se på overvågning således er et eksempel på den sociologiske tilgang hertil. Overvågningssamfundets overvågning er med andre ord et nedarvet biprodukt og ikke en egentlig intenderet konsekvens af informationsberigede processer eller procedurer. Ydermere har den moderne stats ønske om at etablere en korrekt identitet af individer heri været central og set som et middel til blandt andet at opretholde offentlig sikkerhed. Et typisk eksempel i denne forbindelse er et pas, hvor formålet netop er at etablere en sådan korrekt identitet af et subjekt (Stalder

& Lyon, 2003, s. 77-78). Identifikation kan også komme til udtryk på anden vis, idet identifikation er blevet et grundlæggende krav for at kunne klare sig i et moderne samfund. Eksempelvis er det at blive spurgt om ID en helt naturlig del af livet og blot prisen for at leve i et moderne, digitaliseret samfund. Dette er også et eksempel på mange individers store velvilje i forhold til overvågning: Som Lyon påpeger, så fisker vi gerne et ID-kort op af lommen, hvis vi bliver bedt herom (Lyon, 2014, s. 73-74).

Umiddelbart kan man godt få den fejlagtige (og lettere paranoide) opfattelse, at overvågningssamfundet er én stor, homogen "maskine", der indsamler informationer om os alle, hvilket Rule (1973) refererer til som *total surveillance society*. Total surveillance society indebærer: "[...] a single system of surveillance and control, and it's clientele would consist of everyone." (Rule, 1973, s. 37).

Et sådant samfund må være det mest ekstremt tænkelige scenarie (Rule, 1973, s. 37), som man dog ikke møder, og ifølge Rule er det heller ikke forventeligt (1973, s. 37). Rule påpeger, at hvis vi ser tegn på denne form for overvågning, er der i virkeligheden tale om, at det er en afgrænset gruppe, der overvåges i et begrænset stykke tid (Rule, 1973, s. 37). Overvågningssamfundet er således konstitueret af utallige domæner, for hvilke det gælder, at det er forskellige parter[48], der overvåger og bliver overvåget og dette med varierende formål (Lyon, 2007, s. 25, 44). Det er på et mere generelt plan langt fra kun den offentlige sikkerhed, der her er formålet. *Dataveillance* og *big data* sættes også ofte i forbindelse med kommercielle interesser og markedsføring (PRISE, 2007, s. 64). Ræsonnementet bag megen kommerciel overvågning er, at jo

[48] Overvågning i dag har udviklet sig til en industri, hvor eksempelvis såkaldte *information resellers* lever af at indsamle data, behandle disse og videresælge dem. Der kan være tale om data, der er indsamlet af det offentlige og gjort tilgængelige, data hentet online eller data fra andre private firmaer (PRISE, 2007, s. 64). Data kan inkludere navne, telefonnumre, fysiske adresser, IP-adresser , som en bruger har tilgået, data fra sociale medier som Facebook, Twitter, Youtube, kundeklubber, interesser og så videre. Disse firmaer leverer data til et bredt spektrum af kunder, herunder offentlige instanser (United States Government Accountability Office, 2013, s. 2, 4). Det væsentlige ved den type af firmaer er, at digitale databaser med information om personer er selve forretningen og det produkt, der sælges (Nissenbaum, 2010, s. 45).

flere data, man har til rådighed om sine kunder, desto bedre kender man dem. Denne ide er afsættet for en række af de helt store kommercielle succeser: Det klassiske eksempel herpå er Amazon.com, der foretager sofistikeret analyse af data til at skabe en profil af sine kunder. Efterfølgende kan de foreslå produkter, der med stor sandsynlighed matcher de enkelte kunders ønsker, og dermed forsøge at "overtale" kunderne til at købe produkter. En tredjedel af Amazons salg er resultatet af sådanne personaliserede anbefalinger (Mayer-Schönberger & Cukier, 2013, s. 52; Nissenbaum, 2010, s. 29; Ball, Lyon, Wood, Norris, & Raab, 2006, s. 8).

Orienteringen mod forskellige domæner og sammenkørslen af data fra forskellige domæner, der ligeledes er en af de centrale muligheder med *big data*, eksplicitеres også i den måde, politiets arbejde i dag understøttes af software. New York Police Department har i samarbejde med Microsoft udviklet *Domain Awareness System*, der døgnet rundt sammenkører data fra Manhattans 3000 overvågningskameraer, automatiserede nummerpladelæsere, personbårne strålingssensorer og en række andre politidatabaser (The City of New York, 2012). Et sådant masseovervågningssystem kan kortlægge sammenhænge mellem steder, objekter og personer i realtid og dermed være med til at forudsige kriminalitet. Disse data kan nu blive forstået på måder, der tidligere ikke var mulige, og sammenhænge, der tidligere ikke var påviselige, kan nu erkendes.

Man kan i den forbindelse overveje, om sådan masseovervågning uden konkret mistanke betyder, at man betragter individer som skyldige, indtil det modsatte er bevist i forsøget på proaktivt at komme sikkerhedstrusler til livs. Det vil i så fald være et problematisk fundament for et retsstat, hvor det modsatte bør være et grundfæstet retsprincip (Smith, 2010; Zedner, 2009, s. 88). Man kan i forlængelse heraf også overveje, om forsøget på at forudsige kriminalitet er en glidebane, der ligefrem kan lede til, at personer kan anholdes, før de overhovedet har gjort noget ulovligt, blot fordi det er sandsynligt, at de snart vil gøre det. Denne diskussion vender jeg tilbage til i forbindelse med *dataveillance* og *predictive policing* i kapitel 7, *Dataveillance af big data som sikkerhedsteknologi.*

3.1.1. FRA TRADITIONEL OVERVÅGNING TIL *NEW SURVEILLANCE*

I nærværende afsnit diskuteres forskellige definitioner på overvågning. Formålet hermed er dels at demonstrere kompleksiteten af overvågning i dag, dels at præcisere den måde, hvorpå overvågning tilgås i afhandlingen.

Lyon (2003; 2007; 2014), som i høj grad har inspireret synet på overvågning i afhandlingen, definerer overvågning som: "[...] the focused, systematic and routine attention to personal details for purposes of influence, management, protection or direction." (Lyon, 2007, s. 14). Lyon påpeger selv, at definitionen er så bred, at der vil være tidspunkter, hvor ikke alle forhold i definitionen gør sig gældende. Formålet med definitionen er dog blot at give et overblik (Lyon, 2007, s. 14). Denne definition indikerer en asymmetrisk magtrelation mellem den, der overvåger, og den, der overvåges. Den overvågende part er tydeligt den, der dominerer i et hierarki. Definitionen indfanger, hvad jeg her vil referere til som "traditionel overvågning". Desuden har Lyon påpeget, at overvågning altid sigter mod et formål (Lyon, 2007, s. 15).

Med *fokuseret*[49] fremhæver Lyon det forhold, at overvågning i sidste ende er rettet mod et enkelt individ og dette individs personlige detaljer. Hvorvidt dette nødvendigvis gør sig gældende, kan man diskutere, hvilket Lyon dog også selv gør opmærksom på. Man kan argumentere for, at eksempelvis *environmental scanning,* der primært er et strategisk værktøj med det formål at få kendskab til trends i fremtiden, er en demonstration af, at det ikke nødvendigvis er tilfældet, at overvågning er rettet mod det enkelte individ, da man her ikke overvåger den enkeltes data. Overvågning af *big data* kan også være en eksemplificering heraf, idet masseovervågning med henblik på ressourceallokering eller som led i strategiske overvejelser spiller en væsentlig rolle. Omvendt kan man overveje, om man i allersidste ende ikke netop har som formål at udpege nogle konkrete personer på baggrund af de data, man her scanner?

Overvågningen i *environmental scanning* er netop fokuseret. Fokus er dog rettet mod såkaldte svage signaler eller indikatorer på kriminalitet. Man kan i

[49] Egen oversættelse af "focused" (Lyon, 2007, s. 14).

forlængelse heraf også argumentere for, at dette falder indenfor, hvad Lyon udpeger med sit næste adjektiv i definitionen, nemlig systematisk[50]. Det forhold, at ordet systematisk indgår i definitionen, betyder, at der hverken tale om spontan eller tilfældig overvågning af personlige detaljer (Lyon, 2007, s. 14). Desuden påpeger Lyon, at overvågning er *rutineopmærksomhed*[51], hvormed han mener, at det er en almindelig og rodfæstet del af vores hverdag i et bureaukratisk samfund, hvori informationsteknologi spiller en væsentlig rolle (Lyon, 2007, s. 14-15). Dette forhold må siges at være højaktuelt, idet overvågning for alvor er blevet en integreret del af det samfund, vi lever i.

Betegnelsen "traditionel overvågning" skal endvidere ses i lyset af, at den implicitte magt i overvågers favør, som Lyons definition knytter an til, i kraft af at formålet blandt andet er beskrevet som *management*[52] og *direction*[53] (Lyon, 2007, s. 14). Dette er ikke længere nødvendigvis til stede, når nogen våger over hinanden nu til dags.

Social overvågning[54] beskriver ifølge Marwick (2012) den form for overvågning, der udspiller sig på sociale medier. Et kendetegn herved er, at magten er stort set ligeligt fordelt mellem de parter, der våger over hinanden (s. 381). Denne overvågning går så at sige "begge veje". Marwick (2012) stiller derfor spørgsmålstegn ved, om der ved social overvågning overhovedet er tale om egentlig overvågning, hvis man tager udgangspunkt i Lyons definition. "Sousveillance"[55] er ligeledes med til at begrunde anvendelse af termen "traditionel overvågning", idet dette begreb udpeger den aktivitet, hvor man overvåger sig selv – også kaldet *quantified self*. Marx (2002) påpeger også, at den traditionel-

[50] Egen oversættelse af "systematic" (Lyon, 2007, s. 14).

[51] Egen oversættelse af "routine attention" (Lyon, 2007, s. 14).

[52] Begrebet er ikke oversat, da der ikke findes en passende dansk betegnelse.

[53] Begrebet er ikke oversat, da der ikke findes en passende dansk betegnelse.

[54] Egen oversættelse af "social surveillance" (Marwick, 2012, s. 378).

[55] "Sousveillance" betyder "overvågning fra neden", idet det franske "sous" betyder "under". Sousveillance er dermed det omvendte Panoptikon, der kan hjælpe individet med at observere dem, der overvåger (Mann, Nolan, & Wellman, 2003, s. 332-333).

le overvågning ikke indfanger såkaldt selv-monitorering[56]. I dag behøver den overvågede og den overvågende således ikke nødvendigvis være to forskellige subjekter eller parter i en overvågningssituation. I Lyons definition er der en implicit forståelse af, at man kan tale om en sådan sondring mellem overvåger og overvågede, hvorfor definitionen i nogle sammenhænge vil bære for meget præg af generaliseringer. Ovenstående diskussion skal ikke opfattes således, at jeg finder, at Lyons definition ikke er anvendelig, men den indfanger dog næppe hele kompleksiteten i overvågning i dag.

Clarke (1988), ophavsmanden til termen *dataveillance*, og Lyon har nogenlunde enslydende definitioner på overvågning. Forskellen består her primært i, at Clarke eksplicit beskriver, hvordan overvågning kan være af flere personer:

> "Surveillance is the systematic investigation or monitoring of the actions or communications of one or more persons. Its primary purpose is generally to collect information about them, their activities, or their associates. There may be a secondary intention to deter a whole population from undertaking some kinds of activity". (Clarke, 1988, s. 499).

Overvågning er her kort sagt opfattet som en systematisk bevågenhed, hvor der indsamles information med det (sekundære) formål at påvirke personer eller grupper.

To år før Foucault udgav "Discipline and Punish: The Birth of the Prison" (Foucault, 1995), publicerede Rule, som er introduceret tidligere, "Private Lives and Public Surveillance" (1973). Her behandles blandt andet den systematiske opmærksomhed, der er rettet mod individer fra staten (Rule, 1973). Rule tager udgangspunkt i en definition på overvågning, der i kraft af orienteringen imod regler og strukturer vidner om det sociologiske afsæt (Albrechtslund, 2008, s. 53). Rule anfører, at:

> [...] surveillance means any form of systematic attention to whether rules are obeyed, to who obeys and who does not, and to how those who deviate can be located and sanctioned. 'Control' means

[56] Eksempelvis graviditetstests og alkoholtests (Marx, 2002, s. 10). Der findes også en massiv mængde apps, hvormed man kan blandt meget andet kan overvåge egen træning, løberuter, puls, spisevaner, kalorieindtag, vægt eller søvn i løbet af natten.

> the application of concrete measures to forestall or discourage disobedience. 'Mass' is used to refer to situations where single institutions address themselves to very large, impersonal, anonymous publics. 'Mass surveillance and control' is thus not meant to carry a pejorative connotation of continuous, close and malevolent monitoring. The closeness and the friendliness with which the systems studied here attend to their clienteles is a matter for study, not something to be assumed in advance" (Rule, 1973, s. 40).

Rule indleder med at påpege, at overvågning er systematisk, hvilket som nævnt også ses i Lyons definition, ligesom Lyons arbejde kan siges at være inspireret heraf. Interessant er det også, at Rule i definitionen understreger, at masseovervågning ikke nødvendigvis er en negativ handling, hvilket flere andre også har anført. Lyon har som nævnt påpeget, at overvågning befinder sig på et kontinuum mellem omsorg og kontrol (Lyon, 2007, s. 14). Denne pointe er væsentlig, og overvågning er i afhandlingen ikke forstået som en handling, stater "gør" mod individer i en ond mening. Afhandlingens genstandsfelt kan tjene til at illustrere denne pointe. Når en stat overvåger individer med henblik på at opretholde offentlig sikkerhed, så er det netop med det formål at passe på såvel individer og som stat. Dette er ikke en negativ handling i udgangspunktet. Der kan argumenteres for, at der er en håndfin grænse imellem overvågning som "someone is watching" og overvågning som "watching out for someone" (Wood & Webster, 2011, s. 156).

3.1.1.1. NEW SURVEILLANCE

Gary Marx (2002) har fremsat kritik af ordbøgers definition på overvågning, idet disse definitioner typisk udpeger den mere "traditionelle overvågning". Marx eksemplificerer dette med en definition på overvågning fra "Concise Oxford Dictionary": "[...]"close observation, especially of a suspected person"." (Marx, 2002, s. 10). I denne tilgang til overvågning lægges særlig vægt på tillid eller mangel på samme: Overvågning udføres af en autoritet på grund af manglende tillid eller for at kunne etablere tillid (Zureik, 2003, s. 37). Marx' påstand er, at man med en sådan definition ikke formår at indfange *new surveillance*, der i dag finder sted. Betegnelsen *new surveillance* bruges til at påpege teknologiens centrale rolle for overvågning (Marx, 2002). Marx finder, at følgende definition derimod indfanger *new surveillance*: "[...] the use of techni-

cal means to extract or create personal data. This may be taken from individuals or contexts." (Marx, 2002, s. 12). Hermed påpeges det også, at man ikke længere kan definere overvågning som et fænomen, der nødvendigvis retter sig mod et enkelt individ, hvilket som nævnt er i modsætning til Lyons definition (Lyon, 2007, s. 14).

Ved både at henvise til personer og kontekster i definitionen af *new surveillance* sikrer Marx at medinddrage det forhold, at man ved *new surveillance* ofte overvåger mønstre i relationer (Marx, 2002, s. 12), hvilket sociale netværksanalyser og datamining er eksempler på. Datamining inddrages senere i afhandlingen og er her beskrevet som en kombination af dataanalyse og brug af avancerede algoritmer, der er et led i en mere omfattende proces: *Knowlegde discovery*. Formålet med knowlegde discovery er at transformere rådata til brugbar information (Monreale, 2011, s. 27).

Med: "[...] technical means to extract or create personal data." forstår Marx vores mulighed for at "gå udover" den information, vi har til rådighed (Marx, 2002, s. 12). Hermed henviser Marx til den synergieffekt, der opstår, og som er en af hovedfordelene ved sammenkørsel og analyse af data. Resultatet er med andre ord større end summen af enkeltdelene. Nissenbaum henviser også til denne synergieffekt, idet hun påpeger, at: "[...] information begets information: as data is stuctured and analyzed it yields implications, consequences, and predictions." (Nissenbaum, 2010, s. 37). *New surveillance* (og dermed også *dataveillance*) er karakteriseret ved at være næsten eller helt usynlig og meget lidt gennemskuelig for de overvågede (Marx, 2002, s. 28-29). Et eksempel herpå er, at man som individ har meget ringe mulighed for at vide, om man bliver overvåget, når man "færdes" online, hvilket bidrager yderligere til det asymmetriske forhold mellem overvågede og overvåger. Som bruger af internettet lægger man eksempelvis ikke mærke til, om der logges metadata som følge af Logningsdirektivet, når surfer rundt online (Lovbekendtgørelse nr. 988 af 28. september 2006).

Der kan herfra ses en parallel til Benthams Panoptikon, der som nævnt er struktureret således, at den overvågede er uvidende om overvågningen

(Bentham, 1843, s. 44). *Dataveillance*, der foregår på internettet, adskiller sig fra Panoptikon på i hvert fald én betydningsfuld måde, hvilket jeg kort vil forklare. I Panoptikon har den indsatte et vindue, som tillader overvågning. Den indsatte vil stedse være bevidst om den mulige overvågning . På internettet er overvågningsmekanismerne endnu mere skjulte, hvilket kan betyde, at man som bruger kan glemme, at man bliver overvåget – det er ydermere uigennemsigtigt, hvad der bliver overvåget.

Interessant er det, som Foucault nævner, at når magten er perfektioneret, som den er i kraft af Panoptikons arkitektur, så bliver udøvelsen reelt overflødig, idet overvågningen alligevel konstant føles – den internaliseres. De indsatte fanges dermed også i en overvågningssituation gennemsyret af magt, som de ironisk nok selv opretholder (Foucault, 1995, s. 201). Denne diskussion vender jeg tilbage til i flere detaljer i næste afsnit.

Overvågning i dag indeholder en betydelig kompleksitet. Af denne grund kan det være vanskeligt at beskrive samtlige måder, hvorpå overvågning kan finde sted, i en meningsfuld definition. Det eneste, der lader til at passe på alle disse former for overvågning, er tillige det mest basale herved, nemlig at holde øje med eller "våge over" – hvilket dog igen kan komme til udtryk på forskellig måde og med varierende formål. Overvågning kan ligeledes forekomme uden at være indlejret i et hierarki og uden at have en særlig magtrelateret ubalance. Overvågningen, som denne afhandling beskæftiger sig med, har dog visse kendetegn. Der er her tale om en mere traditionel "top-down" forståelse af, at "de" overvåger "os" (Lyon, 2014, s. 72, 80). Der findes med andre ord både overvågning, som har relation til en dikotomi omkring stat og individ, og der findes overvågning, hvor dette ikke gør sig gældende. I nærværende afhandling er den magtbalance, der traditionelt er på spil mellem overvåger og overvågede, stadig særdeles interessant, til trods for at den i andre sammenhænge er udvisket.

Hvad der er "driveren" bag overvågning og bag vores velvilje til at deltage i overvågning, kan i det enogtyvende århundrede ofte forklares ved afsæt i et

spektrum fra en *fear factor*[57] til en *fun factor*[58] (Lyon, 2014, s. 74). *Fun factor* udpeger eksempelvis den overvågning, der sker på sociale web 2.0-netværk eller i reality-tv som Big Brother og Robinson Ekspeditionen. Det er dog overvågning drevet af *fear factor*, der er interessant for denne afhandlings genstandsfelt. *Fear factor* blev for alvor relevant i forbindelse med 11/9 2001, men har også været behandlet før som en del af en større risikodiskurs i samfundet – en diskurs der orienterer sig mod fremtiden. Risikosamfundet er kendetegnet ved sin negative logik, fokus på frygt og bedømmelse af risiko på baggrund af probabilistiske analyser (Ericson & Haggerty, 1997, s. 87, 449-450; Lyon, 2014, s. 75). Netop denne tilgang, hvor probabilistiske analyser er centrale værktøjer, finder man også i forbindelse med *dataveillance*. Dette og implikationerne heraf vil jeg diskutere nærmere i kapitel 7, *Dataveillance af big data som sikkerhedsteknologi*.

3.1.2. Overvåger og overvågede: En magtrelation

I en situation, hvor en part overvåger, og en anden part overvåges, kan dynamikken parterne imellem karakteriseres som ulige og præget af magt og dominans i et eller andet omfang (Foucault, 1995; Lyon, 2007, s. 23; Marwick, 2012, s. 380-382; Richards, 2013, s. 1935). *Overvågeren* er i denne afhandling afgrænset til staten eller offentlige institutioner. Den *overvågede* er afgrænset til individ eller grupper af individer.

Typisk vil overvågeren, altså staten, finde sine begrundelser for overvågning i traditionelle utilitaristiske tanker og i ideen *om mest mulig nytte til flest mulige* og dermed også i det klassiske utilitaristiske *nytteprincip*, som Bentham selv benævnte "The Principle of Utility" (Bentham, 2007)[59]. Nytteprincippet blev fremsat af Bentham i bogen "An Introduction to the Principles of Morals and Legislation" og har følgende ordlyd:

> "I. Nature has placed mankind under the governance of two sovereign masters, pain and pleasure. It is for them alone to point out

[57] Begrebet er ikke oversat, da der ikke findes en passende dansk betegnelse

[58] Begrebet er ikke oversat, da der ikke findes en passende dansk betegnelse

[59] Originalkilden blev publiceret første gang 1789.

> what we ought to do, as well as to determine what we shall do." (Bentham, 2007, s. 1).

Det er ligeledes indenfor denne utilitaristiske tankegang, at Benthams fængsel Panoptikon skal forstås, idet designet heraf tillader en særlig effektiv form for overvågning af de indsatte og indebærer en asymmetrisk magtbalance i sin yderste konsekvens (Bentham, 1843).

Set med nutidens øjne synes Panoptikon ikke umiddelbart at være et sted, hvor det vil være videre behageligt at opholde sig. Fængselsstraffen og den overvågning, der kunne have fundet sted her, blev imidlertid anset for en humanisering af straf, da man hermed bevægede sig væk fra at straffe personer fysisk i offentligheden (Foucault, 1995, s. 16). Man gik med andre ord fra pinestraf til forbedringsstraf. Bentham mente, at samfundet kunne "heles" med Panoptikon, som Albrechtslund formulerer det (Albrechtslund, 2008, s. 35). Foucaults pointe var derimod, at Panoptikon var et billede på det, der foregik ude i selve samfundet.

I forhold til den asymmetriske eller ulige magtrelationen mellem overvåger og overvågede har Foucault i "Discipline and Punish: The Birth of the Prison" (Foucault, 1995) analyseret straffens ændring fra den fysiske pinestraf, hvor afrivning af lemmer og halshugning foregik i al offentlighed, til forbedringsstraffen. Ændringen skete fra omkring år 1760 til cirka år 1840 (Foucault, 1995, s. 3-6). Straffunktionens ændring betød, at straf herefter blev et spørgsmål om at tilbageholde personer i en lukket institution. Frihedsberøvelsen blev dermed den egentlige straf, hvilket var i modsætning til tidligere, hvor frihedsberøvelsen blot var en praktisk foranstaltning forud for den egentlig pinestraf, der i kraft af ritualer og dens ceremonielle form kom til at fremstå som et spektakulært teaterstykke af eksemplarisk karakter (Foucault, 1995, s. 9). Pinestraffen blev set som en kvantificering af lidelse, hvor lidelsen skulle stå mål med den forbrydelse, der var begået (Foucault, 1995, s. 32-34).

Closed-circuit television (herefter blot CCTV) eller et sikkerhedstjek i en lufthavn er nutidige eksempler på sikkerheds-teater, der dog ikke involverer pinestraffens fysiske dimension. Interessant er det, at eksempelvis CCTV, der

er særligt udbredt i Storbritannien og samtidig er en teknologi, der skønnes at have betydelige negative konsekvenser for individer i forhold til teknologiens gevinster, netop kan tolkes som et sådant sikkerhedsteater. Det er en eksplicit manifestation af et politisk ønske om, at nogle 'gør noget' for at komme ulovligheder til livs. På samme tid har CCTV vist sig at have en lindrende effekt på selve frygten for kriminalitet (Wood & Webster, 2011, s. 155-156). Overvågning af data i dag kan komme til at spille en lignende rolle som sikkerhedsteater – dog uden den tydelige, fysiske manifestation, som CCTV-kameraet tydeligt er. Et eksempel på ovenstående skete som følge af terrorangrebet i København i 2015, hvor politikere efterfølgende trækker i arbejdstøjet og bedyrer, at nu skal vi indsamle flere data, og at nu skal der gøres noget i kampen mod terror (Regeringen, 2015).

I fængslet Panoptikon er der som nævnt tale om en forbedringsstraf, en usynlig straffunktion og en indirekte kontrol af mere abstrakt karakter. Formålet er således at forandre fangernes sjæl og deres åndsliv – en form for social kontrol. Panoptikon er ifølge Foucault ikke mindre end det perfekte apparat for denne "disciplinerende magt", idet overvågeren med et enkelt blik kan se alt (Foucault, 1995, s. 173).

Den disciplinære magt fungerer som et paraplybegreb for en række af konkrete teknikker, hvormed man kan lede, dirigere og kontrollere andre. Disciplin har tidligere primært hersket i militæret, skolevæsenet, produktionen og klostrene, men er i det 17. og 18. århundrede blevet: "[...] general formulas of domination." (Foucault, 1995, s. 137). I det moderne samfund var den disciplinære magts rolle dermed ikke længere fyrstens ret til at bestyre andres død, som det gjorde sig gældende med pinestraffen. Nu var fokus derimod rettet mod optimering af de forhold, der kunne give liv til kapitalismen (Heede, 2010, s. 41).

Panoptikon og panoptismen, som den bagvedliggende ide kaldes, var dermed heller ikke udelukkende en teknologi, der resulterede i negative forhold. Panoptismen producerede rent faktisk noget. Den producerede dygtige militær-

mænd, vidende studerende, raske mennesker i kraft af hospitalsvæsenet og lovlydige borgere (Albrechtslund, 2008, s. 48).

Foucault bevæger sig i sin analyse af straffen også uden for fængslet og andre institutioner såsom skoler, hospitaler og militære institutioner.[60] Han påpeger således, at straf og disciplinering også får en central placering i samfundet og i relationer mellem mennesker (Foucault, 1995, s. 296). Implementeringen af den disciplinære magt medfører føjelige kroppe[61] for nu at anvende Foucaults egen (oversatte) terminologi. Føjelige kroppe er kroppe, der i overført betydning er blevet gennemsøgt, skilt ad og sat sammen igen (Foucault, 1995, s. 138). Disciplin handler således om inddeling af individer, det vil sige om klassifikation, kategorisering og rangordning (Foucault, 1995, s. 145). Individerne var dermed også på samme tid resultatet af disciplin og genstand for udøvelsen heraf.

Den disciplinerende magtmekanik, der i kraft af Panoptikons arkitektur gør sig gældende, skal opfattes som en politisk anatomi: Den reelle magt ligger i muligheden for at ændre personers opførsel og dermed muligheden for at socialisere dem – i modsætning til tidligere tiders suveræne magt placeret ved eksempelvis en konge i et monarki (Foucault, 1995, s. 137). Disciplineringsmagt hos Foucault skal imidlertid ikke forstås som en størrelse, der eksisterer i sig selv. Begrebet magt er en aktivitet, der indfanger en række komplicerede, underliggende mekanismer og sociale funktioner i samfundet: "Den hierarkiske overvågning"[62], "den rene sanktion" og slutteligt "eksamen"[63], der

[60] Foucault bemærker selv, at: "I shall choose examples from military, medical, educational and industrial institutions. Other examples might have been taken from colonization, slavery and child rearing." (Foucault, 1995, s. 314, note nr. 1).

[61] I den engelske oversættelse benævnes dette "docile bodies" (Foucault, 1995, s. 135).

[62] I den engelske oversættelse benævnes dette "hierarchical observation" (Foucault, 1995, s. 170).

[63] " I den engelske oversættelse benævnes dette "examination" (Foucault, 1995, s. 184). Hvorvidt det danske begreb eksamen er en korrekt oversættelse af det franske "examen", er der uenighed om, idet det franske ord både dækker over "eksamen" og "undersøgelse". Det samme gør sig gældende for det engelske begreb "examination", der ligeledes kan betyde undersøgelse (ordbogen.com, examination)

kombinerer de to førstnævnte mekanismer. Der er tale om tre underliggende mekanismer eller enkle instrumenter, som Foucault selv benævner disse (Foucault, 1995, s. 170).

Panoptikon er et eksempel på "den hierarkiske overvågning" i en perfektioneret udgave, idet et sådan apparat eller maskine, som Foucault benævner dette, er kendetegnet ved, at man kan se alt med et enkelt blik (Foucault, 1995, s. 173). Panoptikon og den underliggende tanke kan måske umiddelbart virke forældet, men samtidigt et der visse ligheder med forhold i dag, hvor der er et presserende ønske om at indsamle kæmpe mængder information. Nogle lande i EU indsamler ligefrem data med afsæt i en antagelse om, at jo flere data, der indsamles, jo bedre kan man løse problemstillinger, samtidigt med at teknologi hertil ofte bliver: "[...] promoted unproblematically as 'the answer' to multiple threats, most recently to the threat of terrorism" (Ball, Lyon, Wood, Norris, & Raab, 2006, s. 30). Logningsbekendtgørelsen er et eksempel på, at en offentlig myndighed indsamler store mængder data, hvilket fremstilles som modsvaret på terror (Lovbekendtgørelse nr. 988 af 28. september 2006).

Det grundlæggende forhold ved indsamling af al information foretaget af en højerestående magt, som det sker i Panoptikon, lader dermed til at komme til udtryk i nutidens samfund – her dog udmøntet i en postmoderne form. Panoptikon skal i afhandlingen forstås som en abstrakt metafor, der repræsenterer et interessant syn på overvågning uden dog ikke at indramme hele kompleksiteten af overvågning i dag. Her skal det dog bemærkes, at Jeffrey Reiman har påpeget, at Panoptikon som overvågningsmetafor er at foretrække fremfor eksempelvis et akvarium, idet Panoptikon netop indfanger et centralt forhold ved overvågning, nemlig at man kun ser en person fra et enkelt perspektiv, hvilket er et særligt problematisk forhold herved (Reiman, 1995, s. 28). Panoptikon synes stadig at have en vis relevans og således ikke fuldstændig *outdated*. Dette kan siges i særlig høj grad at gøre sig gældende i afhandlingens kontekst, idet det ulige magtforhold, som er kendetegnende for Panoptikon, også gælder forholdet mellem stat og individ.

Ydermere forekommer panoptismen som grundprincip at være repræsenteret i dag i form af den ukontrollable og omfattende overvågning, man oplever i overvågningssamfundet, hvor det er uklart om, og i det hele taget hvornår man overvåges. Panoptismen kommer også til udtryk i institutioner, fængsler, skoler, hospitaler og militærbarakker i dag og er materialiseret med netop dette overvågningsprincip som afsæt. I Danmark er Vridsløselille Statsfængsel fra 1859 et tydeligt eksempel herpå.

Foucault har påpeget et interessant forhold, nemlig at Panoptikon er konstrueret således, at det ikke er nødvendigt, at man rent faktisk bliver overvåget. Det er tilstrækkeligt at være bevidst om, at denne overvågning måske forekommer for at opretholde funktionen heraf (Foucault, 1995, s. 201). Dette kan på én gang være det bedste og det mest problematiske ved overvågningens natur. Under alle omstændigheder bliver det med dette i mente vanskeligt at dæmpe de påvirkninger, som overvågning kan sætte i gang i et samfund og et individ. Det er således tydeligt, at det er problematisk at blive overvåget, men også visheden om, at man måske bliver overvåget, er problematisk. Nu til dags kan man overveje, om Panoptikon findes i en digitaliseret udgave, hvor staten og offentlige institutioner befinder sig i observationstårnet i midten og overvåger individers data?

Modsat Bentham, hvis argumenter for overvågning hviler på utilitarismen, vil opponenter imod overvågning typisk ty til argumenter, som er hentet i den deontologiske tradition, og hævde, at overvågning er et udtryk for manglende respekt for individet og samtidigt krænker individets basale frihedsrettigheder. Immanuel Kant (1724-1804) havde netop respekten for det enkelte individ som et omdrejningspunkt, ligesom retten til at være selvlovgivende var et centralt element i hans normative moralfilosofi (Kant, 1781). Dermed bliver det også eksplicit, hvordan Benthams Panoptikon helt grundlæggende er i konflikt med Kants grundsyn, da der ikke er gjort megen plads til individets autonomi i Panoptikon. Det er imidlertid ikke overraskende, idet Kants og Benthams perspektiver på normativ etik netop er kendetegnet ved at bygge på modsatrettede moralske principper.

Brug af overvågningsteknologi er ikke længere forbeholdt kommuniststater og autokratiske regimer, som eksempelvis Kina og Vietnam. I dag er det også demokratisk valgte regeringer, der foretager overvågning med henblik på blandt andet offentlig sikkerhed (Richards, 2013, s. 1937-1938).

Storbritannien, der både er vestligt og demokratisk, nævnes jævnligt som det klassiske eksempel på kameraovervågning, og er ifølge Raguse det sted i Europa, hvor man har flest overvågningskameraer (Raguse, 2008, s. 28). Faktisk har man i Storbritannien 4,9 millioner overvågningskameraer, hvilket svarer til et kamera per 14 individer (European Commission, 2014a, s. 29). I England alene er der lidt under to millioner overvågningskameraer, hvilket svarer til lidt under et overvågningskamera pr 32 indbyggere (Lauritsen, 2011, s. 14). Samtidigt bemærker Lauritsen, at der i Danmark er omkring 350.000 overvågningskameraer, hvilket svarer til et kamera pr 16 indbyggere (Lauritsen, 2011, s. 14). Det skal bemærkes, at de undersøgelser, Lauritsen henviser til, er udført på forskellig vis, og der er tale om en vis grad af skøn (Lauritsen, 2011, s. 14). Men interessant er det, at noget peger i retning af, at Danmark har taget førertrøjen på, når man ser på antallet af overvågningskameraer pr. indbygger (Lauritsen, 2011, s. 14).

3.1.3. Offentligt og privat samarbejde: Deling af data og overvågning

Som nævnt i foregående afsnit er den overvågning, som afhandlingen omhandler, udført af staten eller offentlige organisationer med offentlig sikkerhed som sigte. Skillelinjen mellem overvågning udført af staten og overvågning udført af private firmaer og organisationer er dog ikke længere så rigid som tidligere (Lyon, 2014, s. 80). Førhen var man primært optaget af overvågeren, hvor det var eksplicit, at denne overvåger havde en klart defineret relation til staten. Der kunne eksempelvis være tale om politiet eller fængselsbetjente (Richards, 2013, s. 1940).

I dag er der et andet og langt mere flydende forhold mellem statens overvågning og overvågning udført af private organisationer. Det er dermed også mere komplekst at bestemme, hvem der er den overvågende part, hvilket blandt

andet kan forklares med, at offentlige institutioner i højere og højere grad udliciterer opgaver til private virksomheder (Ball, Lyon, Wood, Norris, & Raab, 2006, s. 36).

I England vandt IBM tilbage i 2004 eksempelvis kontrakten på "Project Semaphore", som var første fase af et større e-Border-projekt. Dette e-Border-projekt skulle integrere forskellige databaser, der indeholdt data om flypassagerer i forbindelse med indrejse til og udrejse fra England. Data herfra skulle endvidere sammenkøres med biometriske data[64] ved hjælp af et andet projekt, "Project Iris". Formålet var at knytte information om personer med unormal opførsel sammen med biometrisk information (Ball, Lyon, Wood, Norris, & Raab, 2006, s. 37). Det tidligere omtalte "Domain Awareness System" er ligeledes opstået som et samarbejde mellem en privat og en offentlig institution: Microsoft og New York Police Department (The City of New York, 2012).

I en dansk kontekst kan forholdet mellem offentlige og private institutioner eksemplificeres med teleudbyderes indsamling af data for at honorere kravet i Logningsbekendtgørelsen (Lovbekendtgørelse nr. 988 af 28. september 2006). Det er helt konkret de private teleudbydere, der står for dataindsamlingen, men det er staten, der har adgang til og gør brug af disse data til efterforskning og retsforfølgning[65] (Lovbekendtgørelse nr. 988 af 28. september 2006, kapitel 1, § 1.). Således bliver teleselskaberne "gatekeepers" og administratorer i "krigen mod terror".

Der kan endvidere konstateres en tendens til, at stater rundt om i verden i højere og højere grad gør offentlige data tilgængelige for private i digitaliseret form. I nogle sammenhænge benævnes denne praksis *Open Government Da-*

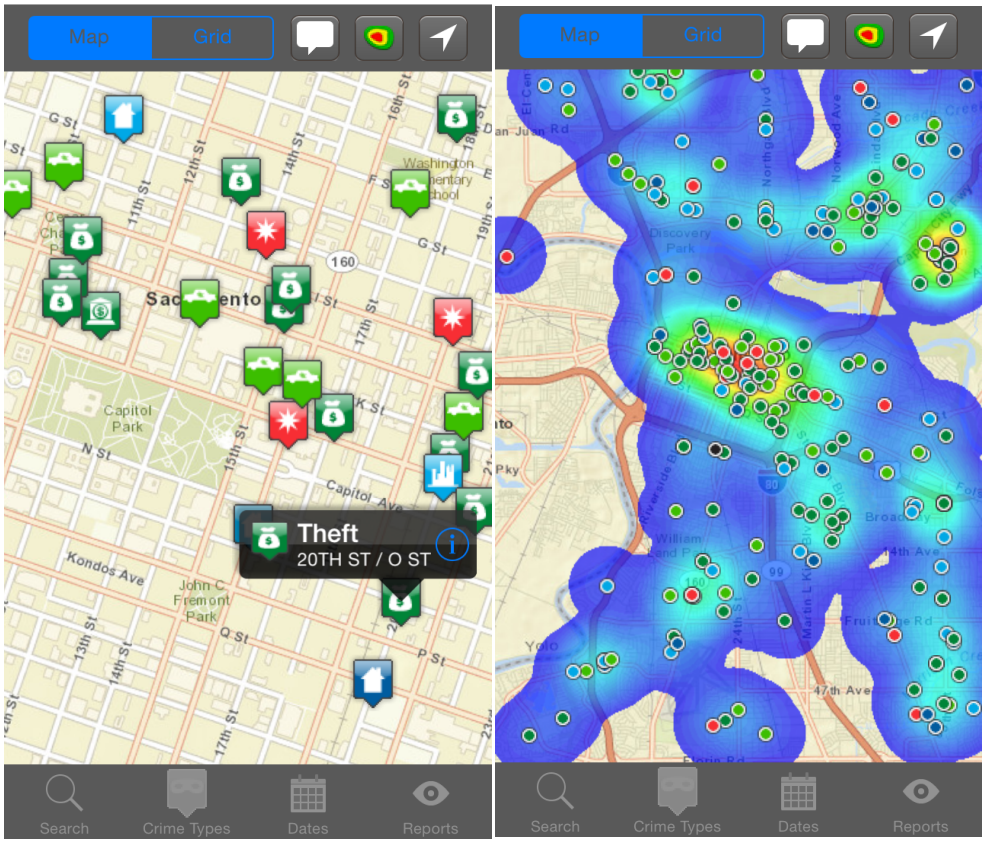
[64] Datatilsynet definerer biometri således: "Biometri er den samlede betegnelse for en række teknikker til identifikation og genkendelse af personer ved hjælp af unikke biologiske kendetegn hos personerne." (Datatilsynet). Der kan her blandt andet være tale om iris- og retinagenkendelse, finger- og håndaftryk, DNA og ansigtsgenkendelse.

[65] I bekendtgørelsen er det fastsat, at: "Udbydere af elektroniske kommunikationsnet eller -tjenester til slutbrugere skal foretage registrering og opbevaring af oplysninger om teletrafik, der genereres eller behandles i udbyderens net, således at disse oplysninger vil kunne anvendes som led i efterforskning og retsforfølgning af strafbare forhold." (Lovbekendtgørelse nr. 988 af 28. september 2006, kapitel 1, § 1.).

ta[66], der er et af de teknologiske forhold, der er med til at skabe den voksende mængde *big data* (Houses of Parliament. Parliamentary Office of Science & Technology, 2014). Et amerikansk initiativ findes på www.data.gov, der er en del af Barack Obamas tiltag om *open government*. Initiativet blev officielt, da Obama i 2009 underskrev "The Memorandum on Transparency and Open Government", der ifølge Obama skal styrke demokratiet og øge effektiviteten gennem transparens, samarbejde og deltagelse (Bauer & Kaltenböck, s. 9; Obama). Ideen med www.data.gov er konkret den, at offentlige data udstilles og kan anvendes til forskning, udvikling af applikationer, forretningsformål, digital datavisualisering og så videre. Siden hen har 46 andre nationer tilsluttet sig Obamas nu globale initiativ. Grundlæggende er ideen med Open Government Data at give fri adgang til data, der ikke er personfølsomme, således at disse data kan anvendes i andre sammenhænge med henblik på at skabe mere viden.

Et konkret eksempel på brug af data fra www.data.gov er et såkaldt kriminalitetskort, der er udviklet med henblik på dels at øge sikkerheden blandt individer, dels at reducere kriminalitet. På kortet kan man orientere sig om kriminel aktivitet i en række udvalgte amerikanske byer. Der gives desuden mulighed for at blive alarmeret via mails, ligesom der er udviklet en applikation til iPhone, hvormed man kan få information om bestemte kriminalitetsformer i selvvalgte geografiske områder. Nedenstående billede 3 er et eksempel på visning af data hentet med denne applikation. Eksemplet er fra Sacramento, Californien.

[66] Begrebet er ikke oversat, da der ikke findes en passende dansk betegnelse.

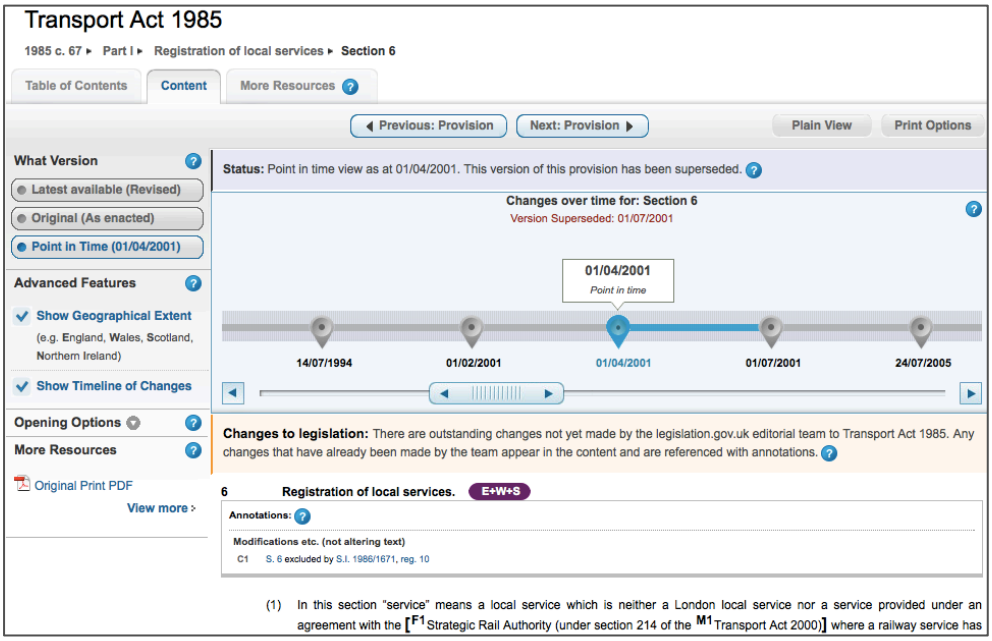


Billede 3: To forskellige visualiseringer over udvalgte kriminalitetsformer i Sacramento, Californien.

Danmark, der er et af de førende lande, hvad angår adgang til offentlige institutioners data, igangsatte i 2009 projektet "Offentlige Data i Spil" (også kaldet ODIS) (Bauer & Kaltenböck, s. 13). Projektet tager afsæt i en grundlæggende tanke om, at man i den private sektor kan anvende offentlige data i kombination med private data, som igen kan bruges til udvikling af nye digitale services, produkter, analyser og så videre (Digitaliseringsstyrelsen, 2013).

I europæisk sammenhæng findes portalen Publicdata.eu, der er en del af et EU-finansieret forskningsprogram, hvor officielle åbne dataset med relation til EU er fremstillet og kan anvendes af private. I Storbritannien har man på www.legislation.gov.uk gjort 800 års lovgivning nemt tilgængelig for borgere, firmaer og andre interesserede. Siden er udnævnt til et *best practice*-eksempel på *Open Government Data*. Udnævnelsen er blandt andet begrundet med, at indholdet findes i en række forskellige standarder. Det er derfor muligt for den helt almindelig web-bruger at tilgå disse data, ligesom Web 3.0-pionerer

frit kan anvende disse data i andre sammenhænge (Bauer & Kaltenböck, s. 50-51). På www.legislation.gov.uk er det nemt at få overblik over ændringer i den enkelte retskilde over tid og se, i hvilket geografisk område i Storbritannien denne retskilde er gyldig. Dette ses i nedenstående billede 4.



Billede 4: Visualisering af Transport Act 1985
(http://www.legislation.gov.uk/ukpga/1985/67/section/6/2001-04-01?view=extent&timeline=true)

Nutidens symbiose mellem overvågende parter betyder ifølge Richards (2013), at det ikke længere vil være meningsfuldt at diskutere og analysere overvågning med en fuldstændig adskillelse mellem statslige og private aktører som overvågere (Richards, 2013, s. 1941-1942). Relationen mellem overvåger og overvågede kan karakteriseres som mindre rigid end tidligere.

I forhold til nærværende afhandling er det dog stadig hensigtsmæssigt at opretholde en sondring mellem overvågning, der er foretaget af henholdsvis offentlig og privat instans, selvom denne opdeling ikke længere er knivskarp. Til trods for at det er private organisationer som eksempelvis teleudbydere, der foretager den konkrete indsamling af data i forbindelse med Logningsbekendtgørelsen, er det stadig et offentligt initiativ, der administrativt og juridisk har igangsat denne dataindsamling. Det er også offentlige institutioner, der har muligheden for at gøre brug af disse data i efterforskningssammen-

hæng. Dermed er det dog ikke sagt, at blot fordi dette initiativ kommer fra en offentlig instans, så er det problemfrit. Den logning, som teleselskaberne har været pålagt, er endvidere blevet kritiseret for at være konkurrenceforvridende. Telebranchen har vurderet, at der er blevet brugt cirka 100 millioner kr. på at indrette systemer til logning. Derudover er de årlige driftsomkostninger anslået til cirka 50 millioner kr., hvilket er en udgift af betydeligt omfang (Institut for Menneskerettigheder, 2015, s. 16). Richards pointe er dog stadig væsentlig at have i mente (Richards, 2013, s. 1941-1942), og udviklingen afstedkommer en interessant dynamik mellem offentlige og private institutioner.

3.2. OVERVÅGNING: IMPLIKATIONER FOR STAT, SAMFUND OG INDIVID

I nærværende afsnit vil en række forskellige implikationer, der menes at følge af såvel overvågning generelt som af *dataveillance*, blive præsenteret og diskuteret. At individets privathed kommer under pres, er en blandt flere grunde til, at overvågning problematiseres, hvorfor privathed også delvist belyses i nærværende kapitel. Det skal bemærkes, at privathed også behandles i kapitel 4., *Informationel privathed,* og kapitel 5., *Databeskyttelse: Retskilder og etikkens berettigelse.*

I nedenstående behandles konsekvenser af overvågning for en række forhold, der er betydningsfulde for stat, samfund og individ. Indledningsvist vil overvågningens konsekvenser blive diskuteret i lyset af social kontrol. I forlængelse heraf diskuteres det, hvordan overvågning kan give anledning til en socialisering af individer, og hvilke implikationer overvågning har for individets intellektuelle privathed. Ydermere diskuteres overvågningens følger for individets autonomi og anonymitet. Slutteligt behandles overvågning i lyset af den kategorisering af individer, der i dag forekommer ved anvendelse af *dataveillance*.

3.2.1. SOCIAL KONTROL

Den teknologiske udvikling og de store mængder data, der indsamles i dag, betyder, at der potentielt kan udøves såkaldt social kontrol med individer. Ball et al påpeger, at social kontrol i nogle tilfælde er: "[...] the strict regulation of personal behavior to order society [...]" (Ball, Lyon, Wood, Norris, & Raab, 2006, s. 33). Den sociale kontrol, der forekommer i vestlige samfund som en del af overvågning, er dog ikke en intenderet del heraf. Derimod er der tale om en utilsigtet og indirekte opstået konsekvens (Ball, Lyon, Wood, Norris, & Raab, 2006, s. 33).

Utilsigtet og indirekte social kontrol kan illustreres med overvågning af undergrundssystemet i London ved hjælp af et såkaldt "Intelligent Pedestrian Surveillance" system. Formålet hermed er at støtte de personer, som sidder og følger med i, hvad CCTV-kameraer optager, og hjælpe med at "få øje på" mistænkelig adfærd blandt de rejsende. Dette gøres konkret ved, at man modellerer, hvad man kan karakterisere som en normal adfærd. Adskiller en persons adfærd sig nok herfra, er denne person mistænkelig. Her tænkes eksempelvis på adfærd, der kan lede til selvmord eller ulovlig indtrængen (Hogan, 2003). På samme måde er intentionen med Londons udgave af det danske Rejsekortet, *Oyster card,* at få flest mennesker hurtigt igennem det offentlige transportsystem og dermed udgå menneskemylder (Ball, Lyon, Wood, Norris, & Raab, 2006, s. 33). *Oyster card* leverer information, der kan afsløre mønstre blandt de rejsende. Det kan dreje sig om, hvor lang en rejse typisk er, hvilke stationer der er de mest anvendte, og på hvilke tidspunkter flest rejser med tog. Denne information kan så danne grundlag for at forbedre og effektivisere togtrafikken (Wood & Webster, 2011, s. 160).

De data, som ligger til grund for ovennævnte forbedringer, er indsamlet om individer og siden samlet i datasæt. Der kan argumenteres for, at såfremt formålet er at bruge disse data til at se mønstre ved personers brug af offentlig transport, er det ikke nødvendigvis problematisk for individet. Men at indsamle disse data giver dog omvendt muligheden for at "zoome" ind på den enkelte, hvilket kan give et omfattende indblik i et menneskes liv (Wood & Webster,

2011, s. 160).[67] Senere i afhandlingen vil en række tilgange, hvorom det påstås, at de kan være med til at løse denne problemstilling, blive inddraget. Her kan igen drages en interessant parallel til Foucaults ide om den normaliserende sanktion, som her kommer under massiv teknologisk indflydelse: Hvis man falder uden for "det normale", må der være noget på færde, som i Foucaults terminologi skal kontrolleres og straffes.

Om disse eksempler fra London er et udtryk for social kontrol, der i en eller anden grad kompromitterer den enkeltes mulighed for at bevæge sig frit og anonymt igennem byen, eller om initiativerne blot er effektivitetsfremmende foranstaltninger og promovering af sikkerhed som et fælles gode, er et spørgsmål om, med hvilke briller man ser.

Der kan argumenteres for, at der i Londoneksemplet netop er tale om en mild grad af social kontrol, idet man her gør brug af en form for regulering af personers opførsel – man forsøger at kontrollere individerne. Dette stemmer også overens med Rules måde at definere social kontrol som: "[...] a single centre attempts to assert it's domination over these elements or, by destroying the old structures themselves, over the people who had comprised them." (Rule, 1973, s. 21).

Omvendt kan man argumentere for, at social kontrol ikke *nødvendigvis* er problematisk i enhver sammenhæng. I forhold til eksemplet må det som udgangspunkt siges at være hensigtsmæssigt, at man forsøger at skabe et større og mere glidende flow i trafikken i en storby. Hvorvidt social kontrol er problematisk, må derfor være afhængig af graden af den konkrete sociale kontrol og måden, hvorpå denne kommer til udtryk. I stedet for at problematisere overvågning i forhold til social kontrol *per se* bør den enkelte(s) situation vurderes. I nogle tilfælde kan man sige, at der blot er tale om en eller anden grad af indflydelse på en person, hvilket kan være helt uproblematisk. Nissenbaum har i den forbindelse også bemærket, at:

[67] Det skal bemærkes, at det ikke forekommer sandsynligt, at det er et funktionelt krav, at man behandler data om hverken personer eller grupper.

> "It would be absurd to insist that only the person who is utterly impervious to all outside influences is truly autonomous; the person would simply be a fool. Although the line between morally acceptable an unacceptable ways of shaping, manipulating, and influencing people's actions is a find, even fuzzy one, the destinction is nevertheless real and worth insistent probing." (Nissenbaum, 2010, s. 83).

Social kontrol og de mekanismer, der her er på spil, er også for Foucault helt centrale emner. Den tidligere beskrevne disciplinære magt er netop et udtryk for en grad af social kontrol og dermed en måde, hvorpå man kan beherske mennesket (Foucault, 1995, s. 137). I tråd hermed har Rule påpeget, at den, der ønsker at opretholde social kontrol, må sørge for blandt andet at opretholde såkaldt *powers of control*[68] (Rule, 1973, s. 22). Dette betyder i praksis, at man skal have mulighed for at iværksætte sanktioner, som kan være negative eller positive, fysiske eller symbolske og formelle eller uformelle (Rule, 1973, s. 22). Jeg finder, at denne måde at forstå sanktionering på i nogen grad stemmer overens med den disciplinære magts mekanismer, da disse i sidste ende handler om det samme, nemlig at kontrollere individet.

For nu at vende tilbage til Foucault sker der desuden en "afinstitutionalisering" af de føromtalte disciplinerende mekanismer og den korrektionsproces, der er indlejret heri, i det 17. og 18. århundrede. Dermed flyttes den sociale kontrol ud i hele samfundslegemet. Magten og den sociale kontrol, der dermed gennemsyrer samfundet og bevæger sig frit heri, hersker som et sandhedsregime, der definerer normalitet. Dette er i modsætning til tidligere, hvor disciplinen og kontrollen primært herskede i relativt lukkede institutioner som fængsler, skoler, militæret og produktionen. Således dannes, hvad Foucault betegner "the disciplinary society" – det socialt kontrollerende samfund, hvis konsekvens er det socialiserede individ (Foucault, 1995, s. 193, 209-211).

For Foucaults er den afinstitutionaliserede, disciplinære magt ydermere kendetegnet ved ikke at blive udført af en dominerende agent, men som noget alle "påfører" hinanden. Denne disciplineringsproces sker på en særlig snedig måde, idet subjektet for den sociale kontrol også bliver en uvidende aktør i denne

[68] Begrebet er ikke oversat, da der ikke findes en passende dansk betegnelse.

proces i kraft af den internalisering af samfundets normer og den socialisering, der sker. Individet bliver med andre ord både genstand og instrument for denne disciplinære magtproces (Foucault, 1995, s. 170-171). Resultatet er det socialiserede individ.

Social kontrol er anset for at være en naturlig konsekvens af det moderne samfund – i hvert fald når dette forekommer i mild grad. Og dermed er det heller ikke problematisk i sig selv. Men det kan uden tvivl anvendes på problematiske måder.

3.2.2. SOCIALISERING OG TRUET INTELLEKTUEL PRIVATHED

Socialisering eller mainstreaming som konsekvens af overvågning hviler på den antagelse, at individer forandres, når de overvåges. Individer opfører sig, som de tror, de bør opføre sig – med andre ord et socialiseret eller mainstreamet individ (Foucault, 1995; Peissl, 2003; Richards, 2013).

Socialisering af individet er hos Foucault et særligt væsentligt område, og det er som nævnt et af tre simple instrumenter, som den disciplinerende magt består af. Normaliseringsmagten er kendetegnet ved, at den straffer forhold med afsæt i egen understrafferet. Der er så at sige tale om en "mini-domstol", hvis formål er at straffe alt det, som er afvigende fra normalen. Det, som kan straffes for at være afvigende, er på en og samme tid kunstigt og naturligt skabt. Kunstig idet det er en orden, der er fastsat ved en lov eller ved et reglement. Det naturlige består omvendt i, at disse love eller reglementer beror på naturlige iagttagelser, såsom hvor lang tid en given øvelse tager at udføre (Foucault, 1995, s. 179). Hvis man som individ honorerer det, som anses for normalt, vil man blive belønnet. Hvis ikke vil man blive straffet, og derved vil personer fornemme de "fejl", de har begået – om disse fejl så er i forhold til tid, væremåde, aktivitet, tale eller krop (Foucault, 1995, s. 177-179)

Det er væsentligt for udøvelsen af normaliseringsmagten at markere afvigelser, kvaliteter og kompetencer og at fremstille hierarkier. Dette sikrer, at individet konstant underkastes et socialiseringspres. Socialiseringspresset betyder i praksis, at alle kommer til at ligne hinanden (Foucault, 1995, s. 181). Hvis man godtager Foucaults ide om sammenhængen mellem overvågning og soci-

alisering, og at dette foregår i hele samfundet som små skjulte mekanismer, så kommer det overvågede samfund til at bestå af individer, hvor afvigelser fra det normale er en sjældenhed. Der gennemtvinges med andre ord en homogenisering af individer.

Til trods for at Benthams drøm om Panoptikon aldrig blev materialiseret, så kan dette bygningsværks idegrundlag og lignende mekanismer i form af observation, der leder til socialisering, også siges at være på spil i nutidens samfund i en digitaliseret form. Baggrunden for, at Panoptikon aldrig blev bygget, var ikke, at Panoptikon hvilede på en utiltalende ide om totalitær overvågning, men derimod at Bentham ønskede, at fængslet skule drives af private kontraktholdere – med ham selv som den første, der kunne skabe profit i kraft af det arbejde, som de indsatte skulle udføre (Albrechtslund, 2008, s. 46; Bentham, 1843, s. 47-51). Interessant er det også at bemærke, at der på den italienske ø Santa Stefano står opført et fængsel, som blev bygget i årene fra 1795 til 1797 og har været i anvendelse helt fra til 1965. Der er interessante arkitektoniske ligheder mellem fængslet på Santa Stefano og Panoptikon. Ideen til Panoptikon blev som sagt udviklet i 1791, hvilket vil sige 4 år før, man påbegyndte Santa Stefano-fængslet. En af tre hypoteser om inspirationen til fængslets konkrete designplan er, at denne er inspireret af Panoptikon. En anden mulig forklaring er, at man har ladet sig inspirere af en tidstypisk, italiensk teaterarkitektur. Den sidste hypotese udpeger ideen, at fængslet er inspireret af et specifikt teater i Napoli, der blev opført i 1737. Under all omstændigheder synes fængslet at være en eksemplificering af Benthams model – om end der ikke nødvendigvis er en faktisk sammenhæng mellem ide og konstruktion (Branco, 2010).

Billede 5: Santo Stefano (https://it.wikipedia.org/wiki/Repubblica_di_Santo_Stefano)

I dag kan socialisering som en konsekvens af overvågning også problematiseres i lyset af den manglende transparens, der omgiver *dataveillance*. Ligesom i Benthams Panoptikon så ved vi ikke nu til dags, hvornår vi overvåges, men muligheden foreligger principielt mere eller mindre konstant. Hermed et det også muligt for individet at blive "et tilfælde" uden at være vidende herom, når det nu ikke er eksplicit, hvornår overvågning finder sted. Den konstante overvågning af individer må nødvendigvis tage afsæt i mistro og mistillid fra det offentliges side. Var mistillid ikke til stede, ville overvågning i en grad som i dag ikke finde sted. Sociale relationer bygger på tillid og: "[...] permitting ourselves to undermine it in this way seems like slow social suicide." (Ball, Lyon, Wood, Norris, & Raab, 2006, s. 3).

Af socialiseringen kan også følge, at individet implicit fratages sin autonomi, hvilket kommer til at udgøre et helt grundlæggende problem for staten og samfundet, idet autonomi er nødvendig for at opretholde et velfungerende, levedygtigt demokrati. Dette forhold vender jeg tilbage til. Samtidigt er en vis grad af variation mennesker imellem en nødvendighed for, at et samfund kan udvikle sig. Der bliver således tale om, at mangfoldighedens muligheder begrænses af socialiseringen.

Overvågning og den deraf affødte socialisering kan således i større eller mindre grad betyde, at et samfunds udvikling stagnerer (Peissl, 2003, s. 22; van Loenen, Groetelaers, Zevenbergen, & de Jong, 2007, s. 146). Dermed kan det også konkluderes at være en misforståelse, at det udelukkende er fordelagtigt for staten at overvåge individer (Regan, 1995).

I forlængelse af Foucaults ideer om normalisering argumenterer Neil Richards for, at en af farerne ved overvågning er, at vores såkaldte *intellektuelle privathed*[69] trues (Richards, 2013). Richards syn på intellektuel privathed hviler på ideer om retten til basale rettigheder som frihed og autonomi og skal her opfattes i bredeste forstand som det at tænke og det at forstå verden. Vigtigheden af intellektuel privathed er baseret på det synpunkt, at: "[...] free minds are the foundation of a free society [...]" (Richards, 2013, s. 1946). Denne ide blev dog for alvor problematiseret i England, da pigen Samina Malik blev tiltalt for terrorangreb, idet hun i 2008 havde downloadet en række bøger om bombefremstilling og en al-Qaeda-manual. Malik blev dømt i byretten, men efterfølgende frifundet i landsretten. Den danske professor i retsvidenskab Eva Smith påpeger i den forbindelse, at dette er et særdeles spinkelt grundlag at rejse tiltale og fælde dom på (Smith, 2010). Smith eksemplificerer dette med, da hun som ung jurastuderende lånte Adolf Hitlers bog "Mein Kampf" af ren og skær interesse og med et ønske om at blive mere vidende om fortiden (Smith, 2010). I dag påpeger hun, hvordan hun ville overveje en sådan handling, hvis det havde handlet om en interesse for al-Qaeda, da dette kan anspore eksempelvis den danske efterretningstjeneste til forkerte ideer om hende. Særligt kan dette problematiseres i lyset af retsstaten, hvor det grundfæstede princip som allerede nævnt bør være, at man er uskyldig til andet er bevist. Som Smith nævner, så kan dette ende med et princip, der siger, at man er skyldig, indtil man har bevidst det modsatte (Smith, 2010). Bliver denne påpasselighed med at opsøge viden en grundfæstet ide i en større befolkning, får samfundets udvikling problematiske vilkår, og det samme gælder individers udvikling (Smith, 2010).

[69] Egen oversættelse af "intellectual privacy" (Richards, 2013, s. 1947).

Man kan i forlængelse af ovenstående hævde, at studerende, der i dag skriver projekter om eksempelvis al-Qaeda eller Islamisk Stat og derfor ihærdigt googler løs på sådanne emner og ser Youtube-videoer med jihad-krigere, måske skal være mere påpasselige i fremtiden. Eksemplet illustrerer, hvordan den intellektuelle privathed og retsstatens principper er nødvendige for et levedygtigt og demokratisk samfund. At individet bør have mulighed for at udvikle egne ideer og meninger uden at andre følger med heri, medmindre individet selv ønsker dette, er væsentligt. Dermed er det ikke sagt, at staten aldrig må foretage såkaldt intellektuel overvågning af individer. Det er blot væsentligt at holde sig for øje, hvilke potentielle konsekvenser en sådan handling kan have.

Denne diskussion problematiserer også direkte EU's ønske om proaktivt at bremse kriminalitet, før den sker. Indsamler man for meget information, har vi netop set, hvad konsekvenserne kan blive. Indsamler vi for lidt information, kan den uønskede skade potentielt ske. I fald man overvåger og dermed risikerer at give den intellektuelle privathed svære kår, så skal man holde sig for øje, at det er en alvorlig trussel mod individers rettigheder og på sigt samfundets eget fundament (Richards, 2013, s. 1951).

Som det blev demonstreret ovenfor, er overvågning en trussel mod staten og samfundet selv. Overvågning af individets intellektuelle privathed kan eksempelvis have den virkning, at tanker om kultur og værdier bliver en "top-down"-proces, hvor sådanne tanker bliver "presset ned over hovedet" på individet. Det bør foregå som en "buttom-up"-proces fra individ til samfund, idet konsekvensen ellers vil være et samfund, der stagnerer. Richards påstand er med andre ord, at kompromittering af intellektuel privathed kan betyde, at individer bliver kedelige, og mainstreaming opstår: Hvis vi bliver overvåget, mens vi foretager os noget intellektuelt, vil vi afholde os fra at foretage os noget, som andre kan synes er afvigende i den ene eller anden forstand (Richards, 2013, s. 1948).

Foucault ville beskrive denne proces som et led i normalisering (Foucault, 1995, s. 177-184). Reiman har i lighed med Foucault argumenteret for, at

normalisering vil ske, hvis vi er under konstant overvågning. Reiman, der har defineret privathed som "[...] *the condition in which others are deprived of access to you*." (formatering i originalkilde) (Reiman, 1995, s. 30), opererer med fire begreber, der samlet kan beskrive den risiko, der er forbundet med at være synlig og mangle informationel privathed: *extrinsic loss of freedom*, *intrinsic loss of freedom, symbolic risks* og *psycho-political metamorphosis* (Reiman, 1995, s. 34).

Extrinsic loss of freedom indebærer, at ens opførsel kan kontrolleres af andre som en konsekvens af manglende privathed (Reiman, 1995, s. 35). Dette gælder, som flere andre har påpeget, såvel hvis man tror, man bliver overvåget, som hvis man rent faktisk bliver overvåget (Benn, 1984; Bentham, 1843; Foucault, 1995). Hvis man ønsker at gøre noget, som er socialt uacceptabelt, eller har nogle overbevisninger, som ikke deles af hovedparten af befolkningen, så kan et socialt pres betyde, at man afholder sig fra den påtænkte aktivitet, eller at man nedtoner sine holdninger. Spørgsmålet er nu, om personer med en stærk psyke kan modstå et sådan socialt pres? Og svaret er ligetil. Man behøver privathed for at kunne udvikle et sådan personlig styrke, og privathed er *a school for character* (Reiman, 1995, s. 37).

Intrinsic loss of freedom betyder, at privathed ikke blot er et middel til at opnå frihed – privathed er med til at konstituere frihed (Reiman, 1995, s. 37). Hvis der ikke eksisterer privathed omkring en persons information, så risikerer denne person at blive frataget nogle valg. Personen er således ikke længere fri. Privatheden er nødvendig for at kunne have valg (Reiman, 1995, s. 37).

Symbolic risks betyder, at privathed er et socialt ritual, hvormed man kan vise andre, at man opfatter dem som ejer af sig selv, af deres tanker og krop. Hvis man ikke tillader folk privathed, tillader man heller ikke folk at eje sig selv. Det er uværdigt og en fornærmelse – en person bliver reduceret til at være en anden persons data (Reiman, 1995, s. 38-39).

Det sidste begreb er P*sycho-political metamorphosis*[70] hvormed Reiman beskriver det forhold, at hvis en person udsættes for konstant overvågning, så vil dette individ blive hæmmet i såvel handlinger som tanker, og man fastholder også personen på et barnligt stadie (Reiman, 1995, s. 40-42). Desuden kan man påpege, at hvis man er under udbredt observation, hvilket eksempelvis kan ske, når myndigheder indsamler data online, så virker det rimeligt at antage, at disse data skal bedømmes i forhold til nogle formentligt ukendte kriterier. Spørgsmålet er nu, om eksempelvis brugere af nettet vil turde at søge på nøjagtigt det, som de har lyst til? Eller om man er bange for, hvilke konsekvenser det kan have, hvis man opsøger bestemt information?

Blot det at vide, at man muligvis er udsat for overvågning, kan betyde, at man opfører sig som om, man overvåges (Bentham, 1843; Foucault, 1995). Ses den problemstilling i lyset af nutidens overvågning af data online, kan det som bruger være svært vide, om man bliver overvåget. NSA-skandalen er også et eksempel på, at blot fordi en person ikke ved, at overvågning af personen pågår, eller at det ikke er offentlig kendt, at der overvåges online, så kan man ikke slutte sig til, at overvågning ikke finder sted.

Et interessant spørgsmål i forlængelse af omtalen om skjult overvågning er, om den ensretning af individer, som overvågning er mistænkt for at medføre, overhovedet vil forekomme, hvis individer er helt uvidende om, at overvågning finder sted? Anede personer ikke, at de blev overvåget, eller måske blot var ligeglade hermed – hvis man havde opfattelsen af, at man var autonom - ville hele denne problemstilling så i virkeligheden blot eliminere sig selv? Min påstand er her, at det næppe er tilfældet. Man kan argumentere for, at hvis man bliver overvåget eksempelvis i en samtale, og man er vidende herom, så vil dette ændre: "[...] ens selvopfattelse og relation til verden [...]" (Ploug, 2003, s. 77). Thomas Ploug (2003) har påpeget, at sådan overvågning kan lede til en mere formel kommunikation i en samtale og måske lede til ændrede synspunkter eller begrænsninger i betroelser (2003, s. 77). Såfremt man ikke er vidende om, at man bliver overvåget i en samtale, vil disse ændringer ikke

[70] Begrebet er ikke oversat, da der ikke findes en passende dansk betegnelse.

træde i kraft. Ploug påpeger, at ens handlinger i så fald ikke vil have de tilsigtede betydninger (s. 77). I sådanne tilfælde kan man kan tale om, at overvågning vil være en umoralsk handling udført af den, der overvåger.

Desuden er det, som Richards også bemærker, ikke sandsynligt, at noget overvågningsprogram vil forblive ukendt. For det andet er det, som allerede demonstreret, ikke kun den intellektuelle privathed og risikoen for mainstreaming, der er på spil i forbindelse med overvågning (Richards, 2013, s. 1952-1953). Så selvom man antog, at man ville løse problemstillingen i forhold til mainstreaming som en konsekvens af overvågning, så ville andre problemer stadig kunne opstå. Eksempelvis kan man argumentere for, at individets autonomi ville have problematiske levevilkår (Kupfer, 1987). Hvis man er under konstant overvågning og dermed ingen privathed har, så bliver det også særdeles problematisk at have sociale relationer.

3.2.2.1. AUTONOMI OG ANONYMITET

Overvågning *kan* skabe en række problematiske vilkår for grundlæggende menneskelige værdier som autonomi og herunder også retten til at være anonym (Ball, Lyon, Wood, Norris, & Raab, 2006, s. 38). Det er en gængs opfattelse, at netop anonymitet er en væsentlig ret i et moderne liv. Ball et al anfører, at anonymitet giver mulighed for frit at skabe egen identitet gennem handlinger og gennem relationer til andre personer (Ball, Lyon, Wood, Norris, & Raab, 2006, s. 38).

Joseph Kupfer (1987) beskæftiger sig ligeledes med autonomi, men i relation til privathed. Kupfer finder, at privathed som instrumentel værdi skal ses som en nødvendig betingelse for, at individet kan udfolde sig som et autonomt menneske, idet han skriver, at: "[...] that privacy is a necessary condition for something of a basic value – the development of an autonumous self." (Kupfer, 1987, s. 81).

Kupfer karakteriserer det autonome individ som et menneske, der selv kan beslutte egne handlinger og selv forme sit liv og herunder også udforme sin livsplan. Udformning af denne livsplan medfører, at individet kan projicere sig selv over i en række mulige fremtidsscenarier. Det er ifølge Kupfer en nød-

vendighed, at individet har en forståelse af sig selv som værende autonom. Kun hvis individet opfatter sig selv som fri til at handle, vil denne proces kunne finde sted (Kupfer, 1987, s. 81). Individet skal med andre ikke blot være fri fra andres kontrol, men også selv forstå at dette rent faktisk er tilfældet. Privathed understøtter hele denne proces, idet det er privathed, der tillader individet at kontrollere, om andre har adgang til dem fysisk og psykisk (Kupfer, 1987, s. 82).

Om det tidligere omtalte London-eksempel, der omhandlede "Intelligent Pedestrian Surveillance"-systemet, kan man også påpege, at netop overvågning i store byer i dag problematiserer det forhold, at man tidligere har kunnet være anonym sådanne steder. At "forsvinde i mængden" var bogstavelig talt en mulighed. Dette stod i kontrast til mindre samfund, hvor den sociale kontrol i højere grad kunne mærkes, og hvor anonymitet ikke kunne udfoldes i samme grad. I mindre samfund kendte alle simpelthen alle.

I store byer er muligheden for fuldstændigt at forsvinde i mængden ikke længere den samme, hvis det overhovedet er muligt. Dette forhold kan tilskrives anvendelse af teknologi i forbindelse med overvågning (Ball, Lyon, Wood, Norris, & Raab, 2006, s. 38; Lyon, 2007, s. 115; Nissenbaum, 2010). I mindre samfund spredes rygter og sladder mellem små sociale grupperinger, og individets fortid er nærmest et fælleseje. Samtidigt kan man dog også argumentere for, at der er en form for tillid og tryghed i mindre samfund, eftersom samlivet og dermed også kontrollen af hinanden foregår mellem mennesker, der kender hinanden, og ikke blandt individer, der oplever overvågningen som noget, der udøves fra "oven" som en automatiseret proces. Den magtbalance, der ses i overvågningen mennesker imellem, kan sidestilles med den magtfordeling, der udspiller sig på de sociale medier i den forstand, at der også her er tale om to parter, der stort set er sidestillede.

Rule påpeger også, at størrelsen på et *socialt miljø*[71] er afgørende for, hvor levedygtig den sociale kontrol er (Rule, 1973, s. 27). Dette skal ses i det lys, at vi har været vidne til et forandret forhold mellem overvågede og overvåger,

[71] Egen oversættelse af social setting (Rule, 1973, s. 27).

eller med Rules egne ord: "[...] changes in the scale of social life have drastic effects on the relations between agencies of control and their clients." (Rule, 1973, s. 27).

Til trods for at et uformelt "alle kender alle"-princip hersker i mindre samfund, er den sociale kontrol og overvågningen radikalt anderledes i dag – og dette både i form og omfang (Lyon, 2007, s. 76, 100; Rule, 1973, s. 27). Man ved simpelthen ikke, hvem der "har noget på en", hvad dette eventuelt måtte være, og hvornår man egentlig overvåges. Transparensen af overvågning er med andre ord ikke særlig stor. Den manglende transparens for de overvågede er af Bentham fremhævet som særligt fordelsagtigt ved Panoptikon, idet det dermed giver grobund for internalisering af netop overvågning (Bentham, 1843, s. 44-45). Dette forhold belyser netop også, hvorfor det er problematisk at udføre overvågning uden mulighed for, at den overvågede har indblik heri.

Endnu en betydningsfuld forskel mellem mindre samfund og større byer er, at i mindre samfund kendte alle hinanden i en eller anden sammenhæng - en social kontekst. Her var der tale om et gensidigt kendskab, hvor man i højere grad får kendskab til et helt billede af en person. Man kan forestille sig, at en sådan gensidighed ikke nødvendigvis har været distribueret fuldstændigt lige. Men forholdet mellem et individ og et andet individ er trods alt mere lige end forholdet mellem et individ og en computer – under alle omstændigheder er det anderledes.

Med databasens indtog kommer det gensidige element i kendskabet til hinanden under pres. Hermed er det billede, der er af den enkelte heller ikke forankret i en social kontekst på samme vis som tidligere (Regan, 1995, s. 223). Der er nu tale om et billede af den enkelte, der er fragmenteret og atomiseret. En forskellighed består i, at man med en database ikke kan skabe det hele billede af et individ i en kontekst (van den Hoven, 1997, s. 37).

Et andet væsentlig forhold er, at en computer principielt kan huske alt for evigt og dette med alle ønskelige detaljer. Det er i modsætning til et menneske, der har begrænset hukommelse og denne hukommelse har i øvrigt en begrænset detaljeringsgrad. Som tidligere nævnt har vi i dag nærmest uendelige

mængder digital lagringsplads til rådighed, hvilket betyder, at behovet for at slette data selvsagt ikke er presserende. Hermed er magtbalancen også tydeligt forskellig, afhængigt af om en computer overvåger et menneske, eller om der kun er mennesker involveret i processen.

Identitet er nært forbundet med autonomi. Identitetsskabelse og identitetsudfoldelse hos individet er ensbetydende med autonomi, hvilket Kupfer som nævnt tidligere i nærværende afsnit har påpeget (Kupfer, 1987, s. 81). I afhandlingen forstås ved det autonome individ kort sagt et individ, der selv bestemmer over eget liv og foretager egne valg. Hvad der kræves for, at man reelt træffer egne valg, er en omfattende filosofisk diskussion, der falder udenfor afhandlingen. For nu er det rimeligt at anvende disse begreber i en almindelig dagligdags opfattelse heraf.

Identitet og autonomi er således retten til selv at definere, hvem man er, hvad man vil, hvem man holder med og så videre. Data, som kan forekomme at være helt ubetydelige i én sammenhæng, kan i kombination med andre data pludselig give "mening". Dermed kan subjektet parkeres i en bestemt kategori (Lyon, 2007, s. 100-101). Der kan være tale om, at det er et misvisende billede af, hvem personen er. Denne bekymring kan mere konkret eksemplificeres med et studie, der omhandlede personlige præferencer, som i større eller mindre grad lod sig forudsige af "Facebook-likes", detaljerede, demografiske data og resultater fra en række psykometriske tests. Der var blandt andet tale om etnicitet, religiøs og politisk overbevisning, intelligens, seksuel orientering, glædesniveau og om, hvorvidt testpersonens forældre var skilt inden dennes enogtyvende år (Kosinski, Stillwell, & Greapel, 2013). Der er tale om information, som i hvert fald i den vestlige verden anses for at være af privat karakter. Der findes divergerende opfattelser af, hvad der er privat information, hvilket jeg vil diskutere i kapitel 4., *Informationel privathed.*

Den viden, som man nu kan "trække" ud af andre informationer, kan give problemer for individets mulighed for at være autonom, idet andre kan få et omfangsrigt kendskab til os som individer.

Et andet eksempel på, hvordan data fra Facebook kan anvendes til at få kendskab til ellers ukendte forhold omkring brugere, er beskrevet af al-Saggaf og Islam i et studie, der tager udgangspunkt i åbne Facebook-data fra 616 personer (Al-Saggaf & Islam, 2014). Der gøres i undersøgelsen brug af såkaldt *web content mining*, der er en dataminingteknik. *Web content mining* kan defineres som: "[...] the process of scanning and extracting the content of a web page, i.e. text, pictures, graphs, audio, video, and hyperlinks, to determine the relevance of the content to a search query." (Al-Saggaf & Islam, 2014) Udgangspunktet for indholdsanalysen i det omtalte studie er begreberne "lonely" og "connected" i statusopdateringer. På baggrund af analysen kunne det blandt andet konkluderes, at personer, hvis Facebook-profilbillede kun viser et ansigt eller en hel familie, sandsynligvis føler sig "connected". Det samme gælder for personer, der har et romantisk profilbillede, hvor de eksempelvis optræder sammen med deres partner, og samtidigt ikke afslører information om politisk overbevisning, religion eller arbejde. Personer, der er interesserede i både mænd og kvinder og informerer om deres sproglige kundskaber, er oftest "lonely" (Al-Saggaf & Islam, 2014). En lang række andre sammenhænge blev også kendte på baggrund af analysen.

Allerede i dag er der tendenser i retning af, at vi er gået fra "jeg er" til "du er" eller "du vil komme til" baseret på analyser af *big data* (Richards & King, 2013, s. 43-44). Ifølge Richards og King er der fare for, at man ligefrem kan ende med "du kan ikke" og dermed blive hæmmet af andres viden om en. Konsekvenserne heraf vil i første omgang gælde det enkelte subjekt, men følgevirkningerne vil kunne mærkes på samfundsplan. Det er svært at vide, hvem man er, og hvad man står for, hvis man konstant får af vide, hvordan man er, hvad man står for, og oveni købet også hvordan man bliver.

Hvis vi konstant er udsat for forsøg på at blive puffet i en bestemt retning baseret på, hvem vi er blevet bestemt til at være, så bliver grænsen for, hvornår et valg er ens eget pludselig mere flydende. Individets identitet og egen skabelse heraf lader til at gå tabt (Richards & King, 2013, s. 44). For det liberale demokrati kan man igen påpege, at forudsætningen for dette er det autonome individ, der kan tage beslutninger, der i væsentlig grad beror på frie valg. Det

er også problematisk, hvis vi er under massiv påvirkning (Gavison, 1984; Regan, 1995).

I forlængelse af ovenstående har Reiman bemærket, at der er en forbindelse mellem liberalisme, privathed og demokrati, og at fundamentet for den forbindelse er det autonome individ (1995, s. 42). Den liberale grundtanke er netop funderet på det autonome individ, der, som Reiman påpeger, er i stand til at handle på baggrund af egne principper efter kritisk refleksion (Reiman, 1995, s. 42). Det autonome individ overtager med andre ikke blot andre individers principper. At lade individer foretage sådanne frie handlinger bygger dog på, at individet har et frit rum, som er privat. Liberalismen foreskriver individets mulighed for at forandre sig, hvilket også er fundamentet for et meningsfuldt virke for individet i et demokrati. Uden denne mulighed er demokratiet mindre meningsfuldt (Reiman, 1995, s. 42). Demokratiet bygger på en ide om, at hvert individ skal have frihed til at vælge, men hvis dette valg blot bliver en overtagelse af andres ideer, så er værdien af demokratiet ikke eksisterende. Muligheden for opretholdelse af autonomi spiller med andre ord en stor rolle i samfundet som helhed, og det er dermed ikke blot et spørgsmål om at tilfredsstille et individuelt behov. I et demokrati skal individer kunne deltage i den politiske proces ved at stemme, ligesom de skal kunne udtrykke deres personlige holdninger til politiske spørgsmål. Autonomi er en nødvendig betingelse for et sådan velfungerende demokrati. Demokratiets fundament er med andre ord det autonome og selvbevidste menneske. Privathed er væsentlig i forhold til autonomi, idet privathed giver rum til at turde at foretage upåvirkede valg (Gavison, 1984, s. 369-370; Peissl, 2003, s. 22; Reiman, 1995, s. 42).

Om værdierne privathed og offentlig sikkerhed kan man anføre, at hvis privathed er væsentligt for demokratiets levedygtighed, så undermineres demokratiet, hvis vi man "sælger" privathed for sikkerhed. Van Lieshout et al spørger meget relevant i den forbindelse, om vi ønsker at leve i total sikkerhed i en politistat? (van Lieshout, Friedewald, Wright, & Gutwirth, 2013, s. 124) Konsekvenserne kan være vidtrækkende, og bevidstheden herom bør medføre et ønske om at tæmme nye teknologier og brugen af overvågning generelt.

3.2.3. KATEGORISERING AF INDIVIDER PÅ BAGGRUND AF DATA

En stor del af den dataovervågning, der sker i dag, har til formål at kategorisere individer – af Lyon benævnt *social sortering*[72] (Lyon, 2003). Kategorisering eller social sortering bliver anvendt i stadig højere grad med henblik på at udpege personer eller grupper, som af den ene eller anden grund udgør en risiko. Det handler helt konkret om at adskille den afvigende minoritet fra hele klientellet (Rule, 1973, s. 279). At se overvågning som social sortering ikke kun som en problemstilling, der opfattes og problematiseres i lyset af individets privathed, kan bidrage til at problematisere overvågning i et bredere perspektiv, der knytter sig til et socialt domæne (Lyon, 2003, s. 13). Dette er igen et eksempel på, at afhandlingens perspektiv på overvågning primært er sociologisk.

Grundlæggende er sortering og kategorisering af information en helt naturlig og ikke mindst nødvendig aktivitet for at forstå verden omkring os. Som mennesker foretager vi hele tiden kategorisering af objekter og herunder af andre personer. Hovedformålet med social sortering er at forudsige og forebygge hændelser, undersøge risici og placere individer i forskellige kategorier, som man så efterfølgende kan behandle forskelligt på godt og ondt.

Big datas invasion indebærer i den forbindelse, at der er endnu flere data, der kan danne grundlag for denne kategorisering. Derfor er mulighederne for sortering og dermed også forskelsbehandling for alvor blevet styrket (Dwork & Mulligan, 2013, s. 35). Social sortering anses ikke for at være uetisk i sig selv – det er en nødvendighed at foretage dette som individ. Det er dog muligt at foretage kategorisering på etisk uforsvarlige måder. En direkte konsekvens af kategorisering kan eksempelvis være diskrimination, der ifølge Den Danske Ordbog (ordnet.dk, diskrimination) er defineret som: "forskelsbehandling til ugunst for nogen". Menneskers liv kan således i udtalt grad påvirkes af overvågning (Lyon, 2014, s. 72).

[72] Egen oversættelse af "social sorting" (Lyon, 2005).

Oscar Gandy, der tydeligt er inspireret af Foucault og Bentham, idet hans primære, teoretiske metafor tager afsæt i Panoptikon, har argumenteret for, at overvågning har potentiale til at diskriminere på baggrund af kategorisering (Gandy, 1996, s. 133-134). Egentlig stammer Gandys teori om overvågning fra en kommerciel kontekst, men kan også anvendes til at kaste lys over information som et muligt middel til diskrimination på baggrund af kategorisering i andre sammenhænge. Til trods for at afhandlingen og Gandys teori beskæftiger sig med forskellige temaer, så er der alligevel en række relevante ligheder, idet de begge udpeger en målgruppe på baggrund af data. I Gandys kommercielle ramme er formålet at øge salg, og i afhandlingens ramme er formålet at rejse mistanke (Lyon, 2007, s. 185).

Kernen i Gandys teori er "The Panoptic Sort", der har transformeret relationen mellem køber og sælger til en upersonlig transaktion baseret på og kontrolleret af information:

> "The panoptic sort is a complex discriminatory technology. It is panoptic in that it considers all information about individual status and behavior to be potentially useful in the production of intelligence about a person's economic value. It is discriminatory because it is used to sort people into categories based upon these estimates." (Gandy, 1996, s. 133).

Hovedideen med "The Panoptic Sort" er således at transformere information til brugbar viden, der kan anvendes til at guide udvælgelsen af, hvem der skal inkluderes, og hvem der ikke skal i en given kontekst. Ifølge Gandy kan personlig information anvendes til tre forskellige, men relaterede funktioner i det omtalte panoptiske sorterings-system: *Identifikation*[73], *klassifikation*[74] og *bedømmelse*[75] (1996, s. 135).

Identifikation omhandler behovet for at skabe en korrekt identitet af dem, der handles med, og nu til dags også for at skabe en optegnelse over forbrugerne, som efterfølgende kan anvendes som grundlag for klassificering. Den person-

[73] Egen oversættelse af "identification"(Gandy, 1996, s. 135).

[74] Egen oversættelse af "classification" (Gandy, 1996, s. 135).

[75] Egen oversættelse af "assessment"(Gandy, 1996, s. 135).

lige information understøtter placering af individer i bestemte grupper på baggrund af fælles karakteristika. De klassificeres og bliver dermed til en type. Klassifikation er nært forbundet til magt, idet den viden, som klassifikationen bygger på, understøtter magt. På baggrund af klassifikationen kan bedømmelsen finde sted, og det vil blive fastlagt, hvorvidt personer skal ekskluderes eller inkluderes. I Gandys teori, der er funderet i en kommerciel kontekst, foregår bedømmelsen på baggrund af blandt andet købedygtighed (Gandy, 1996, s. 135-137).

Gandys teori er i høj grad en spejling af Foucaults ide om det eksaminerede individ. Ligesom Foucault har Gandy beskrevet klassificering og på baggrund heraf eksaminering. Hermed henviser Gandy til den usynlige mekanisme, der forbinder den normaliserende sanktion og den hierarkiske overvågning (Foucault, 1995, s. 170). På baggrund af en eksaminering kan individer nu indplaceres i et hierarki. Når man bliver bedømt i juridisk forstand, er man skyldig eller ikke skyldig. Der er tale om en binær forståelse af skyldsspørgsmålet. Når man eksamineres er der derimod tale om en mere finkornet model, hvor man bliver indplaceret i et hierarki.

Hele denne kategoriseringsproces må siges at have undergået nogle særdeles betydningsfulde forandringer, når det pludselig bliver en automatiseret og rationaliseret proces udført af en computer på baggrund af en algoritme. (Lyon, 2003, s. 13, 23). Foucaults begreb eksamen er ækvivalent med Gandys bedømmelse, der udpeger en funktion, hvori det besluttes om subjektet skal in- eller ekskluderes.

Når man klassificerer individer på baggrund af en række informationer om disse individer, er det overvejende usandsynligt, at man med data kan indfange den reelle kompleksitet, som hvert individ indeholder (Gandy, 1996, s. 137). Det er navnlig det moralske aspekt af en dynamisk person, der ikke kan repræsenteres i en database. I en database er der tale om et stilbillede. Det betyder, at der er en reel risiko for, at man fuldstændigt fejlbedømmer et individ, idet man kun tager en lille del af hele individet i betragtning. Her kan drages en parallel til det af Reiman anførte forhold, at Panoptikon er en hen-

sigtsmæssig overvågningsmetafor blandt andet af den grund, at man her ser et individ fra kun én vinkel (Reiman, 1995, s. 28). Yderligere komplekst bliver det at forsøge at indfange en person i en database, da en person netop er dynamisk og forandrer sig over tid (van den Hoven, 1997, s. 37). Man kan argumentere for, at data om en person i en database kan betyde, at det bliver svært at "komme videre" og udvikle egen identitet, fordi man fastholdes af data i databasen.

Benn (1984) har også beskæftiget sig med, hvad der sker, når man (i bred forstand) observerer en person. Det er ofte risiciene for at skade en person, der bringes på banen med henblik på at modsætte sig observation. Men det er ikke den type modargument Benn er efter. Det skal derfor antages, at de data, der eksempelvis indsamles, ikke kan forvolde skade. Benn spørger: "[...] whether anyone is entitled, prima facie, to be private if he chooses, irresptive of what he is about [...]" (1984, s. 225). Hvis svaret er nej, til at der findes en sådan generelt ret, vil det også betyde, at en generel frihed til at observere andre mennesker eksisterer – med mindre der er tale om helt bestemte forhold, der specifikt er private (Benn, 1984, s. 225).

Benns spørgsmål, om hvorvidt vi kan gøre krav på ikke at blive observeret, er direkte relevant for afhandlingens diskussion om staters overvågning af individer. Besvares Benns spørgsmål med et ja, betyder det anerkendelse af det synspunkt, at det principielt er forkert, hvis man bliver observeret (i bred forstand). Hvis man mener, det er forkert at observere andre *prima facie*, kan staters overvågning mere generelt også problematiseres. Det er netop, fordi man har et *prima facie*-princip, at det jo for så vidt er underordnet, hvad formålet med disse data er.

Spørgsmålet er nu, om retten til ikke at blive observeret også gælder i de tilfælde, hvor indsamlet information ikke vil blive brugt til at skade et individ. Hvad er problemet ved at blive observeret, hvis det netop ikke kan skade en? Benn mener, at observation er mangel på respekt for personer. Når man finder sig selv i en situation, hvor man bliver observeret, så bliver man bevidst

om sig selv på en ny måde. Man bliver bevidst om sig selv set fra en andens perspektiv (1984, s. 226-227).

Således hviler Benns princip om privathed på en mere generel grundidé om respekt for personer (Benn, 1984, s. 228). Dette princip tager afsæt i en forståelse af en person som en aktør, der er i stand til at have projekter og vurdere sine præstationer i forhold hertil (1984, s. 228-229). At begribe en anden person som en person indebærer:

> "[...] to see him as actually or potentially a chooser, as one attempting to steer his own course through the world, adjusting his behaviour as his apperception of the world changes, and correcting course as he perceives his errors. It is to understand that his life is for him a kind of enterprise like one's own, not merely a succession of more or less fortunate happenings, but a record of achievements and failures; and just as one cannot describe one's own life in these terms without claiming that what happens is important, so to see another's in the same light is to see that for him at least this must be important" (Benn, 1984, s. 229).

Respekt for andre mennesker betyder, at man står ved og erkender det forhold, at ens handlinger har implikationer for et andet menneske. At et andet individ er til stede betyder, at man som individ er bevidst om dette og også handler med dette som udgangspunkt. Med mindre vi har grund til at observere en person, skal vi undgå at observere (Benn, 1984, s. 229).

Nu kan men jo med rette overveje, om hemmelig observation af et andet menneske ikke kan gå an? I det tilfælde vil en person ikke vide, at personen bliver observeret. Personen kan vel næppe blive påvirket heraf. Det er dog ikke i overensstemmelse med princippet om respekt for personer at narre dem til at tro, at noget forholder sig anderledes, end det gør (Benn, 1984, s. 330). Princippet om respekt for personer kan anvendes som en forklaring på, hvorfor man som individ kan være utilfreds med staters indsamling af data.

Lad os nu vende tilbage til Foucault. Man kan med rette hævde, at vi har bevæget os videre end Foucaults perspektiver, og at der i dag er tale om en større grad af kompleksitet, end hvad Foucault indfanger med eksamensbegrebet. I dag er de forskelle og ligheder, som optræder mellem mennesker, der er ka-

tegoriseret forskelligt, nemlig reduceret til en kode. Der er tale om en automatisering af overvågning med en kategoriserende teknologi. Den teknologiske mediering betyder blandt andet, at processen kan gå langt hurtigere og være langt mere omfattende, ligesom værktøjerne til at foretage denne kategorisering er blevet mere avancerede. I kraft af det tilgængelige datagrundlag kan der foretages langt mere detaljerede kategoriseringer, end det tidligere har været muligt (Lyon, 2007, s. 104, 117). Implikationen heraf er, at nye sociale klasser, der er baseret på algoritmers behandling af data, vil opstå.

Det er relevant at sondre mellem overvågning foretaget af et menneske og overvågning foretaget af teknologi. Et centralt spørgsmål her er, om der er principiel forskel på de to typer overvågning. Ved computerbaseret overvågning er det blot en algoritme, der "ser" ens data, og menneskelig adgang gives først, hvis der er noget af interesse. I forlængelse heraf må man spørge, om der overhovedet kan være tale om, at privathed kommer under pres, hvis det kun er en algoritme, der har adgang til ens data? (Schneier, 2014). Google har eksempelvis fastholdt, at det ikke er et problem, at en algoritme scanner personers e-mails og efterfølgende sørger for, at der bliver placeret reklamer med relevant indhold. Ifølge Bruce Schneier har en af Googles chefer udtalt, at: ""Worrying about a computer reading your email is like worrying about your dog seeing you naked"." (Schneier, 2014). Citatet skal nok først og fremmest ses som et argumentationskneb med latterliggørelse af den bekymring mange har vedrørende overvågning. Det giver selvsagt ringe mening at sammenligne e-mailscanning med nøgenoptræden for sin hund. I næste afsnit accepterer jeg dog citatets præmis og diskuterer udsagnets indhold.

En hund kan ikke for det første ikke lagre alt, hvad den ser, i sin hukommelse. En computer kan lagre al information, og hvis det ønskes, kan computeren lagre dette for altid. For det andet skal det bemærkes, at hvis ens hund ser en nøgen, så er man også sikker på, at denne information ikke forlader hunden. Derudover har en hund ikke den fornødne fortolkningskapacitet, idet den ikke har noget begreb om nøgenhed og privathed. Det forholder sig væsentligt anderledes med en computer. Man har ingen mulighed for at vide sig sikker på, at de data, der bliver indsamlet, rent faktisk ikke bliver set af et menneske nu

eller senere. Dette kan både være som følge af en fejl, et hackerangreb eller en bevidst handling. Men man kan aldrig vide sig helt sikker (Schneier, 2014). Ydermere er der også den situation, hvor en organisation har en juridisk grund til at bede om at få udleveret indsamlet information – og som Schneier fint bemærker: "There isn't a court order in the world that can get that information out of your dog" (Schneier, 2014). Hunden er isoleret fra mennesker i den forstand, at den ikke kan videregive information. Dette er i direkte modsætning til computeren, der er forbundet til mennesket og kan videregive information.

Til trods for at det blot er en algoritme, der kigger med på en brugers gmail eller en hvilken som helst anden tjeneste, så er det ikke uproblematisk. Man er stadig overvåget, og man er stadig usikker på, hvad de ved overvågningen generede data kan bruges til.

3.2.3.1. KATEGORISERING: OBJEKTIVITET OG INFORMATIONEL SKADE

For digital kategorisering er den bagvedliggende algoritme absolut essentiel. Algoritmen er netop midlet til overvågningen, og den former de resultater, man får (Lyon, 2007, s. 100-101). Interessant er det derfor, når kategorisering af data fremstilles som en værdineutral eller objektiv proces med det argument, at denne kategorisering er foretaget af en algoritme. Dette er imidlertid en forsimplet måde at anskue komplekst område, der har et betydningsfuldt teknisk og humanistisk aspekt (Dwork & Mulligan, 2013, s. 35).

Min påstand er her, at kategorisering ved brug af algoritmer *kan være* hverken neutral eller objektiv. Algoritmer bygger i sidste instans på menneskelige valg om den konkrete konstruktion af algoritmen, og implicitte værdier fra designeren kan fremme eller hæmme bestemt anvendelse. Indlejringen kan ske såvel bevidst som ubevidst. Værdier, meninger og retorik, kan nogle påstå, vil være *fastfrosset* i den bag kategoriseringen liggende kode (Lyon, 2007, s. 76; Lyon, 2003, s. 23). Denne påstand skal imidlertid ikke læses som en afvisning af det synspunkt, som jeg tidligere har påpeget, nemlig et interaktionsperspektiv. Teknologi kan netop understøtte eller hindre bestemt anvendelse, men den brug, der sker, afhænger af den person, der anvender en teknologi.

Konsekvensen af den kategorisering, der sker på baggrund af indsamlede data, er med andre ord, at der skabes en mere eller mindre fuldstændig digital skygge af individer. En sådan digital skygge, af Lyon betegnet en *data double*[76], er ej heller en objektiv gengivelse af et levende individ. Derimod er det et udtryk for outputtet fra en algoritme, der fungerer som den utrættelige overvåger (Lyon, 2003, s. 27).

Hvad angår kategoriseringer, er det yderligere problematisk, at når en kategorisering har fundet sted, kan det være svært "at slippe ud" af en bestemt kategori. Som individ kan man dermed stigmatiseres og det måske endda helt uretmæssigt. Kvaliteten og vedligeholdelsen af data, man gør brug af, er i den forbindelse ligeledes helt essentiel. Har man data til rådighed, der ikke er retvisende i forhold til virkeligheden, risikerer man eksempelvis at placere personer i grupper, de ikke tilhører, og følgelig at træffe forkerte beslutninger (PRISE, 2007, s. 61).

Data er også blevet et værktøj i politiets arbejde i forbindelse med ILP og anvendes dermed til at tage informerede beslutninger (Joh, 2014, s. 35). Dermed får information, der er indeholdt i databaser, også en større og større rolle i politiets arbejde. Dette kan betyde, at måden, hvorpå et område er kortlagt i et givent system, der anvendes til at forudsige hændelser, vil have betydning for, hvorledes politiet vil tilgå dette geografiske område (Bacher, 2013, s. 25). De måder, hvorpå personer eller områder kategoriseres, er bestemt af et individ, der har tillagt forhold som race, etnicitet, alder og uddannelsesniveau en værdi, og dette er så efterfølgende i praksis med til at danne grundlag for politiets arbejde (Lyon, 2003, s. 16).

Dataveillance og den kategorisering af individer, der foregår som "risikoreducerende" eller i hvert fald "risikovurderende" teknologi, kan endvidere medføre, at ideen om en moderne, globaliseret verden, hvor man er mobil som individ, udfordres. Ligesom mulighederne for individuel mobilitet har ændret sig, så har mulighederne for overvågning udviklet sig (Lyon, 2003, s. 24-25). Et eksempel herpå er muslimers mulighed for at rejse efter terrorangrebene på

[76] Begrebet er ikke oversat, da der ikke findes en passende dansk betegnelse.

Manhattan i 2001, idet disse alle var udført at muslimer. Dette kan føre til kategorisering af grupper af mennesker helt generelt, fordi de menes "at være farlige". Overvågning kan således siges i nogle tilfælde at ske med stereotypiske antagelser som grundlag. Resultatet kan være racistisk profilering på ulige vilkår (Hiranandani, 2011, s. 1096).

I forlængelse af ovenstående kan det nævnes, at det er muligt at ende på den amerikanske *no-fly list*[77], blot man kender en, der er mistænkt for terror.

Ifølge LA Times er denne *no-fly list*, der er en del af "terrorist screening-database", ikke sikker i den forstand, at man kan risikere at være på denne liste, selvom man ikke er skyldig. Og det kan være særdeles svært at komme af listen, hvis man ved en fejl er havnet herpå (The Times Editorial Board, 2014). Listen bruges blandet andet til at tjekke personer, der søger om permanent ophold eller statsborgerskab i USA. De praktiske implikationer af den sådan liste kan derfor være vidtrækkende, hvis man er endt på listen ved en fejl (The Times Editorial Board, 2014). At optræde på listen kan betyde, at en ansøger bliver en "national security concern", og en ansøgning om enten statsborgerskab eller permanent ophold kan blive afvist eller ende i et sagsbehandlingslimbo (The Times Editorial Board, 2014).

"Krigen mod terror" og nutidens store interesse for risikovurdering i alverdens sammenhænge kan således føre til diskrimination af mennesker i lufthavne, der har krydset bestemte grænser, hvilket Jespersen et al blandt andre har påpeget (Jespersen, Albrechtslund, Øhrstrøm, Hasle, & Albertsen, 2007, s. 117). Ball et al nævner også dette forhold vedrørende kategorisering af muslimer efter 11/9 2001:

> "[...] sorting might possibly have contributed to safety in the air (we shall never know) but it has certainly led to crude profiling of groups, especially Muslims, that has produced inconvenience, hardship and even torture." (Ball, Lyon, Wood, Norris, & Raab, 2006, s. 8).

[77] Begrebet er ikke oversat, da der ikke findes en passende dansk betegnelse.

Citatet og social sortering mere generelt illustrerer ydermere, hvor vakkelvornt et fundament retsprincippet om at være uskyldig, indtil det modsatte er bevidst, hviler på, når vi anvender data til at udføre social sortering af individer. Idet vi placeres i en gruppe, hvis eksistens vi formentlig er uvidende om, risikerer vi at blive mistænkeliggjort – måske endda uberettiget (Lyon, 2007, s. 21). Og netop det at placere personer i grupper er med adgangen til *big data* og med de rette analyseredskaber blevet til en let tilgængelig proces. Vejen til mulig stigmatisering af grupper og personer er dermed ikke så lang.

Kategorisering giver nyt liv til "det digitale b-hold" på en ny måde. Her tænkes ikke på den ulige mulighed mennesker har for at anvende teknologi, men derimod på hvordan kode i dag er grundlag for den prioritering mellem individer, der finder sted. Det er muligt at bestemme, hvor meget "de er værd" og risikovurdere dem på baggrund af alder, race, etnicitet bopæl og så videre. Lyon bemærker, at man som individ vil have uens muligheder i livet, alt efter hvilken kategori man tilhører. I øvrigt er en sådan proces ofte kun kendt af den, der udfører kategoriseringen (Lyon, 2007, s. 101-102).

Der er som nævnt et basalt, menneskeligt behov for at kategorisere. I dag, hvor dette nemt kan gøres i kraft af *big data*, er det nødvendigt med ekstra opmærksomhed herpå og samtidig forholde sig kritisk til de værdier, der er indlejret i denne kategorisering, for at få det bedst mulige resultat og for at undgå de problemer, som kategoriseringen kan give (Dwork & Mulligan, 2013, s. 40).

4. INFORMATIONEL PRIVATHED

4. INFORMATIONEL PRIVATHED

I dette kapitel er informationel privathed omdrejningspunktet. Informationel privathed er netop den form for privathed, der kan komme under pres, når stater overvåger individers data.

Moor har påpeget, at "[...] privacy is like good art, you know it when you see it." (Moor J. H., 1997). Som anført i afhandlingens første kapitel har Thomson bemærket, at det mest påfaldende ved privathed er, at ingen rigtig ved, hvad det er (Thomson, 1984, s. 272). Regan har dog lidt mere optimistisk anført, at privathed er vagt begreb, men at det samme gør sig gældende for begreber som eksempelvis frihed og lighed (Regan, 2011, s. 497).

De fleste vil erklære sig enige i, at privathed har instrumentel værdi (Moor J. H., 1997, s. 28). Jeg vil ikke udfordre denne antagelse. Dog vil jeg påpege, at privathed som instrumentel værdi er en *nødvendig betingelse* for at kunne opnå *betydningsfulde,* intrinsiske goder såsom autonomi , integritet og muligheden for at kunne opretholde sociale relationer (Se eksempelvis: Benn, 1984; Edgar, 2002; Fried, 1984; Gerstein, 1984a; Rachels, 1984).

Solove (2007) argumenterer for en pluralistisk forståelse af privathed. Han bemærker således, at:

> "[...] privacy is not reducible to a singular essence; it is a plurality of different things that do not share one element in common but that nevertheless bear a resemblance to each other." (Solove, 2007, s. 756).

Solove anfører, at privathed skal opfattes som et paraplybegreb for et: "[...] related web of things." (Solove, 2007, s. 760). Formålet med nærværende kapitel er ikke at finde essensen af privathed, og jeg vil tilgå privathed som Solove foreslår, nemlig med en pluralistisk forståelse.

Aktuelle kapitel om privathed består af fire dele: 4.1., *Privathedens semantik*, 4.2., *Perspektiver på informationel privathed ,* 4.3., *Privathed som et fælles gode* og 4.4., *Privathed – "intet at skjule"-argumentet.*

I afsnit 4.1., *Privathedens semantik,* vil jeg indledningsvis diskutere betydningen af begreberne privat, privatliv og privathed. Ydermere vil jeg påpege det problematiske aspekt i en tilgang til privathed, der tager afsæt i en forståelse af, at det, der er privat, er det, andre ikke har interesse i. I afsnit 4.2., *Perspektiver på informationel privathed,* vil jeg behandle privathed i lyset af en række tilgange hertil. Diskussionen er struktureret omkring kontrol versus begrænset adgang til information. Ydermere vil jeg undersøge privathed i forhold til information med afsæt i en kontekstuelt forankret forståelse af, at der ikke er noget, der er privat *per se* – det, der er privat, er netop forankret i en kontekst (Moor J. H., 1997; Nissenbaum, 2010). I afsnit 4.3., *Privathed som et fælles gode,* vurderes privathed med udgangspunkt i et argument om, at privathed ikke kun har værdi for individet, men også for staten og samfundet – et fælles gode. I afsnit 4.4., *Privathed – "intet at skjule"-argumentet,* diskuterer jeg sluttelig "intet at skjule"-argumentet, og hvorfor jeg vurderer, at det er et problematisk argument. Argumentet er centralt at inddrage i afhandlingen, da begrundelsen for, at stater kan overvåge individer, i nogle tilfælde hviler på dette argument om, at det kun er de personer, der gør noget kriminelt, der har noget at skjule. Præmissen for argumentet bygger på den ide, at privathed primært handler om at skjule kriminelle aktiviteter. Det problematiske i den præmis bliver indirekte demonstreret i den pluralistiske tilgang til privathed, og jeg vender tilbage hertil i slutningen af nærværende kapitel.

4.1. PRIVATHEDENS SEMANTIK

Adjektivet "privat" kommer af det latinske *privatus*, der betyder "ikke officiel" (Lund, 2007) eller "adskilt fra det offentlige" (ordnet.dk, privat). "Adskilt fra det offentlige" peger således på, at der må være mindst to forskellige sfærer – en offentlig og en privat[78]. Hensigten med at beskrive informationel privathed[79] som en flersfærisk størrelse er i høj grad at kunne kaste lys over de problemstillinger, der her kan optræde. Dette perspektiv udfoldes i aktuelle kapitel,

[78] Nissenbaum sidestiller privathed med kontekstuel integritet, hvor der dog der tale om en langt mere finmasket model, der ikke kun tager to sfærer i betragtning (Nissenbaum, 2010).

[79] Jeg opfatter her privathed og privatliv som synonymer.

hvor det samtidig påpeges, at det at operere med en offentlig/privat-dikotomi er en forsimpling af virkeligheden. Det er med andre ord ikke tilstrækkelig finmasket til at kunne indfange og karakterisere de forskellige relationer, et individ har, og de sfærer, man som individ agerer i (Regan, 2011, s. 499). En mere finmasket forklaringsmodel i forhold til sfæreperspektivet vender jeg tilbage til (Nissenbaum, 2010; Nissenbaum, 2004).

Eksemplerne på betydningen af "privat" er i Den Danske Ordbog flere, da begrebet kan optræde i en række forskellige sammenhænge.[80] Der kan være tale om en adskillelse af individ og stat, hvilket udtrykkes: "[...] som ikke hører ind under eller angår staten eller det offentlige." (ordnet.dk, privat). Et andet eksempel er: "[...] som (kun) angår eller vedrører en enkelt person eller en lille gruppe af personer, og som ikke vedkommer andre." (ordnet.dk, privat). Dette relaterer sig både til ideen om privathed som noget, der skal ses i lyset af sociale relationer, og til forestillingen om, at nogen er adskilt fra andre – ideen om sfærer er igen til stede.

Substantivet "privatliv" betyder:

> "[...] den del af en persons liv eller tilværelse som ikke vedkommer andre (end nogle ganske få), og som ligger uden for personens officielle funktioner, fx arbejdsmæssige eller politiske især om aspekter der vedrører personens familie, følelser og seksualitet." (ordnet.dk, Privatliv).

Dette er igen er en eksemplificering af ideen om, at der er forskellige sfærer i livet, der er adskilt.

Privatliv oversættes typisk til det engelske *privacy*, hvis betydning blandt andet eksemplificeres med: "A state in which one is not observed or disturbed by other people [...]" (oxforddictionaries.com, privacy) og "The state of being free from public attention [...]" (oxforddictionaries.com, privacy). De engelske betydninger af *privacy* er umiddelbart i overensstemmelse med det danske *privatliv*.

[80] "Privat" kan også anvendes i andre sammenhænge. Eksempler herpå er en privat virksomhed, et privatforbrug og privat i juridisk forstand i forhold til for eksempel staffesager (ordnet.dk, privat).

Ovenstående beskrivelser af, hvad privathed betyder, betoner det forhold, at privathed er svært definerbart. Det er her mere præcist den betragtning, at både privatliv og privathed kan karakteriseres som den del af livet, der ikke "vedkommer andre", der kan diskuteres. Umiddelbart kan det synes at være en hensigtsmæssig måde at identificere kernen i begrebet privathed – altså "den del af en persons liv eller tilværelse som ikke vedkommer andre". Det kan formentlig også rimelig uproblematisk bruges som en operationel, dagligdags måde at forstå privathed. Hvis man underkaster begrebet privathed en systematisk vurdering, kan en sådan forståelse dog kritiseres. Det umiddelbare spørgsmål, man kan stille, er, hvad der så er kriteriet for, hvad der ikke vedkommer andre? Og hvem bestemmer, hvad der ikke vedkommer andre? Hvis det er "de andre", der bestemmer, hvad der ikke vedkommer dem, har det enkelte individ ikke længere indflydelse på, hvad der er privat (Schoeman, 1984, s. 411). Der eksisterer så at sige hverken kontrol med eller begrænset adgang til information om en selv.

Schoeman har påpeget denne problemstilling og illustreret den med et væddemål. Hvis to personer indgår et væddemål om en tredje, og de har brug for en given information for at kunne afgøre deres væddemål, så vedkommer en bestemt information pludselig de to, der har indgået væddemålet (Schoeman, 1984, s. 411). Information, der ikke vedkommer andre, er således problematisk at anvende som kriterium for, hvornår noget er privat.

4.2. PERSPEKTIVER PÅ INFORMATIONEL PRIVATHED

I afsnit 4.2.1., *Privathed som kontrol versus begrænset adgang,* vil jeg indledningsvis diskutere privathed som kontrol over information (Fried, 1984; Warren & Brandeis, 1984) og privathed som begrænset adgang til information (Reiman, 1995). Desuden vil jeg slutteligt inddrage privathed som *kontrol/begrænset adgang*[81], hvilket er Moors måde at kombinere de to nævnte tilgange (Moor J. H., 1997, s. 31). Ydermere vil jeg løbende i diskussionen inddrage blandt andre Rachels (1984) og Gerstein (1984a), idet de har behandlet privathed som betingelse for henholdsvis sociale relationer og intime relatio-

[81] Egen oversættelse af "control/restriced access" (Moor J. H., 1997, s. 31).

ner. Andre centrale begreber i forhold til privathed såsom autonomi og integritet inddrages ligeledes i diskussionen.

I afsnit 4.2.2., *Kontekstuel forankret informationel privathed,* beskrives privathed i lyset af en kontekstuel forståelse, hvorved der også fremsættes et mere nuanceret perspektiv på ideen om privathed som kontrol. Nissenbaum (Nissenbaum, 2010) og Moor (1997) forsvarer antagelsen om, at det, der er privat, har en kontekstuel forankring, hvilket de dog begrebsliggør på forskellige vis og med forskellig detaljeringsgrad. Jeg vil her primært fokusere på Nissenbaums mere veludviklede beskrivelse, der både rummer et deskriptivt og et normativt element (Nissenbaum, 2010).

4.2.1. PRIVATHED SOM KONTROL VERSUS BEGRÆNSET ADGANG

Nogle finder, at det er nødvendigt at have kontrol over information, for at man kan tale om, at privathed er til stede. I opposition til dette synspunkt mener andre, at det er tilstrækkeligt at have begrænset adgang. Denne diskussion om kontrol versus begrænset adgang til information er blevet aktualiseret af den teknologiske udvikling, idet der nu findes midler til at indsamle og overvåge data med eksempelvis sikkerhed som mål.

Forståelsen af privathed som kontrol over information blev grundlagt, da amerikanerne Samuel D. Warren og Louis D. Brandies publicerede den i dag klassiske artikel "The Right to Privacy" i Harward Law Review (Warren & Brandeis, 1984). Hermed lød startskuddet også til den akademiske litteratur om privathed. Siden hen har eksempelvis Fried (1984) forsvaret denne grundlæggende tanke. I opposition til forståelsen af privathed som kontrol over information har blandt andre Reiman (1995) forsvaret privathed som begrænset adgang til information. Reiman tager afsæt i en grundlæggende antagelse om, at kontrol med information grundet teknologi ikke er mulig, hvorfor det er mere realistisk at tale om at ville begrænse adgangen til information. Moor har tilbudt et alternativt perspektiv, hvor han kombinerer ovennævnte to tilgange til information, hvilket han benævner *kontrol/begrænset adgang*-teori. Moor argumenterer således for, at de rigtige personer skal have adgang til vores data på de rigtige tidspunkter. Derudover skal individer have så meget

kontrol over deres information, som det er muligt (Moor J. H., 1997, s. 31). I Moors teori er der således også indlejret en kontekstuel forståelse.

Warrens og Brandies' ide om privathed som kontrol med information tog afsæt i en bekymring om offentliggørelse af information, der tilhører et privat domæne i livet, idet stillbilledkameraet havde set dagens lys (Warren & Brandeis, 1984, s. 76). Stillbilledkameraet i kombination med sladderpressen kunne vise sig at sætte individets privathed under pres:

> "Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that "what is whispered in the closet shall be proclaimed from the housetops."" (Warren & Brandeis, 1984, s. 76).

Warren og Brandies argumenterede for, at der manglede en eksplicit, juridisk beskyttelse af individets privathed, der på det tidspunkt kun implicit blev behandlet i amerikansk lovgivning i kraft af blandt andet ejedomsret og ophavsret (Warren & Brandeis, 1984, s. 76). Dermed kunne en persons privatsfære mod dennes vilje afsløres for offentligheden. Warren og Brandies mente, at individet har en privatsfære, hvor man som individ har: "[...] the right to be left alone;" (Warren & Brandeis, 1984, s. 74). Derfor synes det relevant at undersøge om:

> "[...] the existing law affords a principle which can properly be invoked to protect the privacy of the individual; and, if it does, what the nature and extent of such protection is." (Warren & Brandeis, 1984, s. 77).

Warren og Brandies påpeger, at en persons "[...] thoughts, sentiments, and emotiones [...]" (Warren & Brandeis, 1984, s. 78) skal kunne beskyttes mere hensigtsmæssigt, end de allerede var på artiklens publiceringstidspunkt. Formålet med en eksplicit ret til privathed er at bestemme, i hvilken grad information om en person kan deles. Det grundlæggende princip er en "[...] inviolate personality [...]" (Warren & Brandeis, 1984, s. 85) og "[...] the right to one's personality [...]" (Warren & Brandeis, 1984, s. 83). Denne ret til egen personlighed inkluderer en mere generel ret til immunitet med hensyn til egen personlighed (Warren & Brandeis, 1984, s. 83). Warren og Brandies betoner såle-

des privathed under henvisning til integritet. Integritet kan siges at være en fysisk og mental urørlighedszone, der eksisterer generelt og er således ikke betinget af, at det enkelte individ udtrykker ønske om, at dets integritet respekteres.

Fried (1984) har ligeledes forsvaret privathed som kontrol over information om en selv (Fried, 1984, s. 210). Privathed er af Fried anset som en nødvendig betingelse for at kunne udvikle sig som en person, der kan etablere og bevare intime relationer (Fried, 1984, s. 211). Sådanne relationer vil bygge på respekt, kærlighed, venskab og tillid (Fried, 1984, s. 205). Der er implicit i Frieds opfattelse af privathed tale om en primær interesse for relationen mellem to (eller flere) individer. I lighed med Frieds antagelse, om at privathed er nødvendigt for at kunne udvikle sig som person, har Edgar påpeget, at privathed også handler om muligheden for at kunne trække sig tilbage (Edgar, 2002, s. 255). Vi er som individer konstant "på", og derfor har vi brug for et frirum. Edgar omtaler dette som: "[...] *preservation of mental health* [...]." (Edgar, 2002, s. 255). Også Benn omtaler individets mulighed for at trække sig tilbage og forme sig selv. Kun i det øjeblik, hvor vi er helt fri fra andres bedømmelse og observation, bliver dette muligt. Vi har i Benns terminologi brug for at "[...] drop the mask [...]." (Benn, 1984, s. 241). At tillade et individ denne mentale urørlighedszone, som Benn og Edgar efterlyser, betyder, at individets integritet kan opretholdes og beskyttes. Integritet forudsætter ikke særlige mentale evner – med integritet refererer man til en grundlæggende og konstant respekt for individers ligeværdighed. Det betyder, at retten til integritet ikke er afhængig af, om et individ selv evner at opretholde egen integritet. I modsætning hertil er privathed, der i nogle udlægninger forankres i en ret til selvbestemmelse - autonomi med andre ord.[82] Selvbestemmelse kræver evner til at kunne udleve denne ret. Integritet er uafhængig af evner.

For nu at vende tilbage til Frieds tilgang kan man sige, at denne eksplicit illustrerer et kantiansk inspireret menneskesyn, idet teorien om privathed bygger på en ide om, at mennesket skal have lov til at forfølge det, som det ønsker,

[82] Eksempelvis kræver det at kontrollere eller begrænse information om en selv evner og selvbestemmelse.

og ikke blot være et middel (Fried, 1984, s. 206). Centralt i Kants pligtetik er det netop, at man ikke må behandle et menneske som middel til at opnå et mål, hvilket Kant beskriver således:

> "For rational beings ...every one of them ought to treat itself and all others *never merely as means*, but always *at the same time as end in itself*." (Formatering optræder i originalkilde) (Kant, 2002, s. 51)[83].

At individer aldrig må behandles som et middel til at opnå et mål, er at have *respekt for personer* ifølge Kant. Hermed kan integritet igen fremhæves, idet Kants ide om respekt for personer netop peger på opretholdelse af individets værdighed og integritet. Et individ er uerstatteligt og har indre værdighed (Kant, 2002, s. 53). I lyset af den problemstilling, som behandles i nærværende afhandling, kan statens overvågning af individer problematiseres. Når man bruger overvågning af individer som et middel til at opnå et mål, nemlig offentlig sikkerhed, kan man stille spørgsmålstegn ved, om sådan overvågning lever op til Kants princip om respekt for personer (Edgar, 2002, s. 254).

I lighed med Fried har Gerstein påpeget, at: " [...] intimate relationships simply could not exist if we did not continue to insist on privacy for them." (Gerstein, 1984a, s. 265). Det er problematisk, når man husker, at intime relationer ifølge Gerstein har intrinsisk værdi. (Gerstein, 1984a, s. 268). Privathed er så at sige en nødvendig betingelse for intime relationers eksistens.

Gerstein påpeger endvidere, at såfremt man observerer en anden i den intim situation, er dette problematisk i forhold til den observerede persons autonomi. Dette forhold gør sig gældende, selv om den observerende part føler sympati med og forståelse for den, som er under observation. Gersteins pointerer, at det er forkert at observere en anden mod personens vilje. Som autonomt individ har man ret til selv at bestemme, hvornår man vil observeres (Gerstein, 1984a, s. 267, 270-271).

Ligesom Reiman har Gerstein betonet det forhold, at man som observeret bliver opmærksom på sig selv og sine handlinger. Dette syn er i overensstem-

[83] Originalkilden publiceret første gang i 1785.

melse med Reimans *double vision*, der tidligere er introduceret som en del af et begrebsapparat (Reiman, 1995, s. 38).

Intime relationer er ifølge Gerstein et intrinsisk gode, og privathed er en nødvendig betingelse herfor (Gerstein, 1984a, s. 270). At der sker en eksklusion af personer, der ikke er en del af en bestemt intim relation, er en essentiel del heraf. Gerstein betoner, at privathed ikke er den eneste væsentlige forudsætning for en intim relation – men det er den mulighedsbetingelse, der giver den intime relation et fundament til at kunne leve og udvikle sig (Gerstein, 1984a, s. 271).

Fried har ydermere påpeget, at privathed ikke er fravær af information om individet, som andre vil have kendskab til. Det, som privathed handler om, er derimod, hvorvidt vi har kontrol med den information, der omhandler os selv (Fried, 1984, s. 209). Denne kontrol med information skal ikke opfattes kvantitativt, men snarere kvalitativt. En person kan eksempelvis godt kende til, at en kollega ikke har været på arbejde i en længere periode. Et sådan viden behøver ikke at være privathedskompromitterende. Hvis kollegaen yderligere havde kendskab til sygdommens nærmere omstændigheder, ville det pludselig være noget andet i forhold til privathed (Fried, 1984, s. 210).

Reiman (1995) har kritiseret Frieds syn på privathed som kontrol og er i modsætning hertil af den opfattelse, at privathed er: "[...] the condition in which other people are deprived of access to either some information about you or some experience" (Reiman, 1995, s. 30). De divergerende opfattelser af privathed, der består imellem Reiman og Fried, kan illustreres med et eksempel omhandlende en mand på en øde ø. Spørgsmålet er, om det giver mening at tale om, at en mand på en øde ø har privathed?

Fried ville på dette spørgsmål svare, at det er direkte ironisk overhovedet at tale om, at en mand på en øde ø har privathed (Fried, 1984, s. 210). Manden, der er alene på øen, har ikke har behov for at kontrollere privathed. Der er jo kun denne mand og dermed ikke nogen privathed at kontrollere. Hans problem er måske i virkeligheden det modsatte, nemlig at han har for meget privathed. Ifølge Reiman betyder privathed derimod, at andre er: " [...] deprived

access to you." (Reiman, 1995, s. 30). For Reiman er det meningsfuldt at tale om, at denne mand har privathed. Der er jo netop ikke nogen på øen, der har adgang til manden, og man kan således hævde, at denne mand i allerhøjeste grad er i en situation, der kan rubriceres som privat.

Reiman kritiserer endvidere Frieds argumentation for, at privathed er en nødvendig betingelse for intime relationer mellem mennesker. Reiman finder ikke, at en intim relation bygger på, at de pågældende personer har et gensidigt kendskab. Derimod er det væsentlige i en intim relation, at personerne holder af hinanden (Reiman, 1995, s. 31). Reiman eksemplificerer dette med, at man kan have en intim relation til et andet individ, uden man har udvekslet informationer. Omvendt eksisterer muligheden også for, at man kan dele privat information med en fremmed, uden man har et intimt forhold (Reiman, 1995, s. 31). Et eksempel kan være, hvis man under samtaler med en psykolog fortæller om private forhold. Dette medfører ikke, at man har en intim relation.

Reimans kritik af Fried synes rimelig, og det forekommer problematisk at hævde, at privathed er en *nødvendig betingelse* for intime relationer. Som det er nævnt, så kan en intim relation godt eksistere uden deling af information. Jeg vil argumentere for, at privathed kan have afgørende betydning for at etablere og opretholde *forskellige typer af relationer*, herunder også intime relationer.

Rachels (1984) har påpeget, at vores mulighed for at kunne kontrollere, hvem der har adgang til os som individer og til information om os, har betydning for de sociale relationer, vi indgår i. Privathed er en nødvendig betingelse for, at vi kan opretholde disse forskellige sociale relationer (Rachels, 1984, s. 292-293). Rachels påstand er endvidere, at der er en række mønstre i, hvordan vi opfører os i forskellige sociale sammenhænge og i samvær med forskellige mennesker (Rachels, 1984, s. 293). Rachels påstand forekommer intuitivt rigtig og kan nemt eksemplificeres: En kvinde opfører sig på én måde overfor sine elever, når hun underviser som folkeskolelærer, mens hun agerer anderledes overfor sine egne børn, sin mand, og når hun er sammen med venner. De fleste

kan sikkert også nikke genkendende til, at man optræder anderledes i sociale sammenhænge sammen med sin kæreste, mand eller kone, end når man blot er derhjemme selv (Rachels, 1984, s. 293).

I modsætning til Rachels påpeger Wasserstrom, at interpersonelle relationer kan forbedres, såfremt individer er mindre optagede af at opretholde privathed (Wasserstrom, 1984, s. 331). Ønsket om at opretholde en mere privat side betyder, at individer lever et uærligt dobbeltliv. Man viser én side af sig selv til nogle og deler en anden del af sig selv med andre (Wasserstrom, 1984, s. 331). Det skal bemærkes, at Wasserstrom opfatter privathed som en kulturel norm, med hvilken individer nærmest "spænder ben" for sig selv. Hvis der ikke eksisterede en kulturel norm, der foreskrev, at nogle handlinger ikke bør foretages i det offentlige rum – eksempelvis det at have sex – så ville man i høj grad også fratage andre muligheden for at gøre skade ved at observere personer i den situation. Om man bliver observeret, mens man spiser, gør ikke den store forskel. Det samme princip skal overføres til handlinger, der på grund af kulturelle normer ikke forekommer offentligt (Wasserstrom, 1984, s. 331).

Benn har i overensstemmelse med Rachels' syn betonet det forhold, at man kan tale om *rolle-forventninger* i forbindelse med interpersonelle relationer. Der eksisterer forskellige forventninger til opførsel, alt efter hvilke relation man indgår i som individ (Benn, 1984, s. 235). I lighed med Rachels og Benn mener jeg, at interpersonelle relationer er struktureret forskelligt, og individer opfører sig forskelligt i forskellige sammenhænge. Der er således tale om, at individet er dynamisk. Dermed mener jeg også, at den kritik, der kan fremsættes mod denne position – nemlig at man ikke viser sin "ægte person", eller holder sit "rigtige jeg" tilbage – er fejlagtig (Rachels, 1984, s. 293). Der kan også argumenteres for, at såfremt man gebærder sig på forskellig vis i forskellige sociale sammenhænge, betyder det heller ikke, at man mister integritet eller autenticitet. Man kan navigere i forskellige sociale sammenhænge på samme værdigrundlag som menneske. Og dertil kan man måske også spørge, om det ikke netop er evnen til at gebærde sig forskelligt i uens sammenhænge, der er med til at definere et socialt velfungerende individ? Den forståelse, jeg har argumenterer for, knytter også an til den senere ide om, at man som indi-

vid bevæger sig i forskellige sfærer eller kontekster i livet, hvilket har afgørende indflydelse på privathed.

Rachels opfattelse af privathed kan karakteriseres som en kombination af en kontrolforståelse og en kontekstuel forståelse. Rachels har netop påpeget, at privathed er en nødvendig forudsætning for at kunne opretholde sociale relationer, hvilket indirekte bygger på en ide om, at der er forskellige sfærer i livet, og disse skal kunne holdes adskilt.

Som det er klart nu, har Fried og Rachels argumenteret for, at kontrol med information er helt centralt for at kunne opretholde privathed. Jeg mener dog, at man kan sætte spørgsmålstegn ved, om kontrol med information reelt er en nødvendig betingelse for, at sociale eller intime relationer kan eksistere. Vil det ikke være tilstrækkeligt, hvis man som individ er i en situation, hvor man kan *begrænse information?* Moor har endvidere kritiseret kontrolperspektivet ud fra en betragtning om, at dette i den teknologiske verden, vi i dag befinder os i, ikke længere er levedygtigt (Moor J. H., 1997, s. 31). *Greased data*, et begreb der er introduceret i afhandlingens introduktion, kan ifølge Moor ligeledes forklare, at information er svært kontrollerbar.

Moor fremstiller et syn på privathed, som han kalder *kontrol/begrænset adgang.* Herved advokerer Moor for en begrænset adgang til information, men i de tilfælde, hvor det rent faktisk er muligt at have kontrol med information, er det ifølge Moor ønskværdigt. Teorien er konstrueret således, at Moor får fordelene fra både begrænset adgang-tilgangen og kontrol-tilgangen til privathed (Moor J. H., 1997, s. 31). Grundlæggende er Moors opfattelse af privathed hensigtsmæssig, idet han giver rum for, at forskellige mennesker kan have forskellig adgang til information på forskellige tidspunkter (Moor J. H., 1997, s. 31). Det er ikke relevant at tale om privathed i kontroløjemed på en absolut måde.

På den ene side forekommer det rimeligt, at man som individ selv har kontrol med data omhandlende en selv. I praksis er det dog ikke nogen nem opgave som følge af teknologiens udvikling. Omvendt kan man overveje, om det ikke er problematisk at opgive ønsket om kontrol med information, blot fordi en

sådan kontrol er stedse vanskeligere. Det kan i hvert fald vise sig at være en uheldig glidebane i forhold til beslutninger, hvis vi opgiver vores privathed under henvisning til den teknologiske udvikling.

Spørgsmålet, der også rejser sig, er, om det overhovedet er nødvendigt at have kontrol med information i absolut forstand? Med afsæt i en kontekstuel forståelse af privathed vil jeg argumentere for, at det ikke er nødvendigt at vælge "side" i denne debat (Nissenbaum, 2010, s. 147). Jeg vil udfolde dette synspunkt yderligere i nedenstående.

4.2.2. KONTEKSTUEL FORANKRET INFORMATIONEL PRIVATHED

Jeg vil nu med en kontekstuel tilgang redegøre for og diskutere anvendeligheden af privathed. Løbende i afhandlingen er der argumenteret for, at det er hensigtsmæssigt at forklare privathed med udgangspunkt i en kontekstuel forankring (Nissenbaum, 2010). Information er med afsæt i en kontekstuel forståelse ikke privat *per se*. Om information er privat, afhænger af, hvem informationen deles med, og hvorledes informationen bevæger sig. Kendetegnende for en kontekstuel tilgang til privathed er, at teorier indenfor dette område forstår privathed i lyset af en lokal kontekst (Warnier, Dechesne, & Brazier, 2015, s. 435).

Jeg vil diskutere henholdsvis Moors og Nissenbaums forståelse af privathed i en kontekstuel forankring (Moor J. H., 1997; Nissenbaum, 2010). For både Nissenbaum og Moor er fokus ikke på selve informationen som privat eller offentlig, men på zonen eller konteksten, hvori denne information er tilgængelig. Nissenbaums kontekstuelle forståelse af privathed er dog langt mere finmasket end den, Moor præsenterer. Af samme grund vil jeg primært beskæftige mig med Nissenbaums tilgang.

Moor demonstrerer en kontekstuel forståelse af privathed, idet han opererer med såkaldte *privathedszoner*[84] (Moor J. H., 1997, s. 30). Disse zoner betyder, at kun de rette informationer bliver tilgængelige for de rette mennesker. Informationer, som anses for at være private i én zone, er det ikke nødvendigvis

[84] Egen oversættelse af "zones of privacy" (Moor J. H., 1997, s. 30).

i en anden zone. Moor påpeger også, at hans syn på privathed betyder, at "[...] the notion of privacy really attaches to a situation or zone and not to the information itself." (Moor J. H., 1997, s. 30).

Ideen om, at privathed lægger sig til en bestemt zone, kan illustreres med dagligdags eksempler. Det kan eksempelvis være uproblematisk at tale med sin læge om psykiske problemer, men en kommende arbejdsgiver drøfter man ikke den slags med. Ligeledes kan information om religiøs overbevisning være problematisk i nogle sammenhænge og naturlig i andre. Det er med andre ord ikke relevant at anskue privathed i absolutte termer. Information kan endda være direkte skadende i en zone, men på ingen måde problematisk i en anden zone. Moors privathedszoner er grundlæggende analoge med det, som Nissenbaum navngiver kontekst (Nissenbaum, 2010, s. 132-134).

Den kontekstuelle tilgang til privathed betyder, at vi ikke forpligter os til at have nogle foruddefinerede kontekster eller zoner – for eksempel en privat og en ikke privat. Disse zoner eller kontekster er fleksible og afhænger af den situation, man vil vurdere i forhold til privathed.

I Nissenbaums teori, *kontekstuel integritet,* er *kontekst-relative informationsnormer* omdrejningspunktet (Nissenbaum, 2010, s. 129; Nissenbaum, 2004, s. 119).[85] En kontekst er en sfære i livet (Nissenbaum, 2004, s. 137). Eksempler på kontekster kan være uddannelse, sundhedsvæsen, arbejdsplads og familieliv. Enhver kontekst består af et normsæt, der har forskellig oprindelse (Nissenbaum, 2004, s. 137). Disse normer kan have deres oprindelse i eksempelvis kultur, historie, konventioner eller jura. Normerne har indflydelse på, hvad man bør og ikke bør gøre. Ydermere har disse normer indvirkning på personers indbyrdes roller i en given kontekst.

[85] Nissenbaum behandler i artiklen "Privacy as Contextual Integrity" (Nissenbaum, 2004) og i bogen "Privacy in context Technology, Policy, and Integrity of Social Life" (Nissenbaum, 2010) samme teori om kontekstuel integritet. I bogen præciseres dele af teorien, men efter min vurdering er teorien og ikke mindst de to centrale informationsnormer mere klart forklaret i artiklen fra 2004. Jeg anvender derfor denne som primær kilde til Nissenbaums teori. Det er også i artiklen, at Nissenbaum eksplicit benævner de to informationsnormer, som jeg vil behandle i nedenstående. Jeg vil dog inddrage Nissenbaums bog i det omfang, jeg finder det hensigtsmæssigt.

Med anvendelsen af *kontekstuel integritet* fremhæves det, at integritet er en tilstand, som et individ kan være i, og som lægger sig til en given kontekst. Individets integritet opretholdes, når bestemte informationer ikke er tilgængelige for andre set i lyset af en bestemt kontekst. Den informationelle urørlighedszone, vi ønsker at beskytte, er så at sige forskellig fra kontekst til kontekst.

Nissenbaum introducerer to informationsnormer, der skal opretholdes, for at *kontekstuel integritet* er til stede. Det skal bemærkes, at Nissenbaum sidestiller privathed med *kontekstuel integritet* (Nissenbaum, 2004, s. 138). Kan blot den ene af de to normer ikke opretholdes, er den kontekstuelle integritet ikke længere til stede – og dermed kompromitteres privatheden (Nissenbaum, 2004, s. 143).

Den ene norm benævner Nissenbaum *normen om passende information*[86]. Normen om passende information fastlægger, som navnet indikerer, om en given personlig information er passende eller ikke er passende at videregive i en bestemt kontekst (Nissenbaum, 2004, s. 120). Det er eksempelvis passende at tale med sin læge om sygdom, det er passende at tale med sin bankrådgiver om finansielle emner og privatøkonomi, og det er passende at tale med sin lærer om karakterer. Omvendt vil det i mange sammenhænge være upassende at fortælle kollegaer ved et frokostbord, hvilken medicin man tager. Nissenbaum bemærker dog også, at kontekst-begrebet er fleksibelt, og det er forskelligt, hvor restriktive regler der eksisterer i forskellige kontekster med hensyn til, hvad der er passende information (Nissenbaum, 2004, s. 139). En venskabskontekst er eksempelvis særdeles fleksibel. Det vil variere fra venskab til venskab, hvad der er passende information. Omvendt er en arbejdsplads en kontekst, der er omfattet af et mere restriktivt normsæt for, hvad det er passende at tale om.

Den anden norm, som Nissenbaum benævner *normen om bevægelse eller distribution af data*[87], angår information, der distribueres. Denne norm regulerer

[86] Egen oversættelse af "norms of appropriateness" (Nissenbaum, 2004, s. 138).

[87] Egen oversættelse af "norms of flow or distribution" (Nissenbaum, 2004, s. 138).

så at sige distributionen af information mellem to eller flere parter (Nissenbaum, 2004, s. 140). Det teoretiske afsæt for Nissenbaums teori og herunder særligt *normen om distribution af information* er Michael Walzers (1995)[88] teori om *distributive justice,* der grundlæggende handler om fordeling af goder mellem mennesker (Walzer, 1995, s. 6).

Walzers teori hviler på en antagelse om, at et samfund består af sfærer, og hver sfære er defineret af et socialt gode (Walzer, 1995, s. 6). Et socialt gode kan eksempelvis være arbejde, uddannelse eller penge. Til hver af disse sfærer knytter sig et særligt sæt af retfærdighedsnormer for, hvorledes de sociale goder skal fordeles. I en arbejdssfære tildeles jobs på baggrund af kvalifikationer (Walzer, 1995, s. 145). I en uddannelsessfære gives studiepladser til studerende på baggrund af blandt andet interesse og kvalifikationer (Walzer, 1995, s. 199, 203). Varer distribueres i en handelssfære efter købernes økonomiske formåen (Walzer, 1995, s. 103-104). For at opnå det, som Walzer benævner *kompleks lighed*[89] og dermed retfærdighed, skal de sociale goder fordeles i overensstemmelse med de standarter, der gælder i den enkelte sfære (Walzer, 1995, s. 318).

Nissenbaum argumenterer i overensstemmelse med Walzers teori for, at information skal distribueres i overensstemmelse med gældende kontekstuelle normer (Nissenbaum, 2010, s. 168). I Walzers tilfælde fører dette til retfærdighed og i Nissenbaums teori til integritet (Nissenbaum, 2010, s. 168).

Den grundlæggende ide med de to omtalte informationsnormer er, at:

> "What matters is not only whether information is appropriate or inapproriate for a given context, but whether it's distribution, or flow, respects contextual norms of information flow" (Nissenbaum, 2004, s. 141).

For de to informationsnormer gælder det videre, at de er til stede i alle kontekster. Disse normer er dog ikke absolutte eller universelle – de er *relative* til konteksten (Nissenbaum, 2004, s. 143). Nissenbaum bemærker desuden, at

[88] Originalkilden blev publiceret første gang i 1983.

[89] Egen oversættelse af "complex equality"(Walzer, 1995, s. 318).

privathed som begrænset adgang har elementer fælles med ideen om de to informationsnormer (Nissenbaum, 2010, s. 147). Der er således tale om, at nogle individer på de rigtige tidspunkter kan få kendskab til ens information. Normen om passende information indlejrer også ideen om privathed som kontrol, idet denne norm er bestemmende for, om privathed er passende i en given kontekst, eller om denne information skal kontrolleres (Nissenbaum, 2010, s. 148).

Kontekstuel integritet kan både have en normativ og en deskriptiv rolle. Således kan *kontekstuel integritet* bruges til at udpege, hvor privathed kan komme under pres. *Kontekstuel integritet* kan også bruges som forklaringsmodel for, hvorfor en bestemt situation skaber modstand, og hvorfor en anden situation accepteres, til trods for at man skal afgive information (Nissenbaum, 2010, s. 148).

I den konkrete anvendelse af *kontekstuel integritet* skal man indledningsvis bestemme, hvilken social kontekst der er i spil. Det vil være forskelligt, om det er let at bestemme den sociale kontekst, som netop gør sig gældende (Nissenbaum, 2010, s. 149). Næste trin er at undersøge, om der er nye, centrale aktører på spil med hensyn til, hvem der modtager information, hvem informationen omhandler, og hvem der overfører information (Nissenbaum, 2010, s. 149). Ydermere skal det bestemmes, hvorvidt de forandringer, der måtte være sket, har nogen indflydelse på, hvilke information der overføres fra afsender til modtager. Hvis det er nødvendigt, kan der foretages ændringer i den eksisterende praksis vedrørende overførsel af information fra en part til en anden (Nissenbaum, 2010, s. 149). Såfremt disse ændringer leder til ændringer i praksis, kan det betyde, at kontekstuel integritet ikke kan opretholdes (Nissenbaum, 2010, s. 150).

4.2.2.1. KONTEKSTUEL TILGANG: FORKLARING AF ANOMALIER I PRIVATHED

Kontekstuel forankret tilgang til privathed kan bruges til at forklare anomalier i forhold til privathed (Moor J. H., 1997, s. 31; Nissenbaum, 2010, s. 186-187). Det er netop her, jeg vurderer, at den kontekstuelle tilgang har en af sine mest

fremtrædende styrker i forhold til afhandlingens genstandsfelt. Et simpelt eksempel kan illustrere denne pointe.

Man kan forestille sig en person, der er vældig aktiv på sociale medier. Personen har en blog, hvor hun deler information og tanker om sine børn og sit ægteskab. Disse informationer er tilgængelige for alle, der kommer forbi hendes Facebook-profil eller blog. Informationerne eksisterer i én social kontekst online og er netop også forankret her. Selvom personen selv har gjort disse informationer tilgængelige, kan man stadig forestille sig, at hun vil være utilfreds, hvis disse data blev brugt til et andet formål, end hun havde tiltænkt – eksempelvis hvis disse data gøres til genstand for systematisk overvågning af et statsligt organ.

Sikkerhedstjek, der foregår i lufthavne, kan ligeledes bruges til at illustrere *kontekstuel integritets* styrke. I en lufthavn tillader vi, at vores bagage bliver gennemlyst og måske også gennemsøgt, hvis det skønnes nødvendigt (Nissenbaum, 2010, s. 187-188). Med udgangspunkt i en forståelse af privathed som kontrol så er det klart, at et lufthavnssikkerhedstjek er privathedskompromitterende: Man skal åbne sin taske, pakke relevante dele op og lade tasker gennemlyse. Man har ingen kontrol med sin egen information.

Tager man samme situation i betragtning og forstår privathed som *kontekstuel integritet*, så er der ikke nødvendigvis tale om, at ens privathed kompromitteres (Nissenbaum, 2010, s. 187-188). Vi befinder os i eksemplet i en sikkerhedskontekst. Og såfremt man bringer normen om passende information i spil, så er det netop passende, at der sker et sikkerhedstjek inden en flyvning. I forhold til den anden informationsnorm, nemlig normen om bevægelse eller distribution af data, så bevæger disse informationer om ens kuffert sig ikke ud af den sikkerhedskontekst, der er tale om.

Såfremt man opfatter privathed i en kontekstuel forståelsesramme, så har man en robust forklaringsmodel for privathed, der ikke reducerer privathed til et spørgsmål om kontrol eller hemmeligholdelse af information. Det bliver således muligt at forklare, hvorfor personer deler information og på samme tid værner om deres privathed (Nissenbaum, 2010, s. 187).

En anden styrke ved den kontekstuelle tilgang er, at det forekommer umuligt at udpege nogle informationer som private og andre som ikke private. Privathed som kontrol fordrer, at man bestemmer, hvilke informationer der er private, og hvilke der ikke gør sig fortjent til dette prædikat. De kontekstuelle informationsnormer er netop *kontekstuelle* – de er aldrig universelle, og de er altid bundet til en given kontekst (Nissenbaum, 2004, s. 143).

Hvis man forestiller sig, at man skulle udpege informationer, som altid er private og dermed kan rubriceres som tilhørende en privat sfære, så vil man ende med "laveste fællesnævner". En information som ikke nødvendigvis altid er privat, kan ikke tilhøre denne kategori. Og informationen må således nødvendigvis være "ikke privat". Det forekommer umiddelbart særdeles svært at skulle udpege informationer, som altid er private. I den forbindelse må man spørge, hvilket kriterium der er, for at noget er privat? Hvis man tillader, at en given information er offentlig (og dermed ikke privat), skal denne information så kunne tilgås af alle andre i alle tænkelige sammenhænge? Der viser sig hurtigt nogle omfattende problemer ved at definere informationer ud fra en sondring mellem kun to sfærer. Her viser Nissenbaums og Moors tilgang deres styrke.

4.2.2.2. KRITIK AF DEN KONTEKSTUELLE FORSTÅELSE AF PRIVATHED

De kontekstuelle privathedsnormer, der er nævnt i ovenstående, skal opfattes som fikspunkter for, om privathed kompromitteres eller ikke (Nissenbaum, 2004, s. 143). Det vil således sige, at den nuværende opfattelse af, hvad der er normalt, også bliver den, som ny praksis skal måles og vejes i forhold til med henblik på at bestemme, om en eller flere informationsnormer brydes (Nissenbaum, 2010, s. 158-159; Nissenbaum, 2004, s. 143). Denne tilgang implicerer imidlertid et problem, idet normer er foranderlige.

Det er klart, at det ikke er hensigtsmæssigt at anvende et "moralsk værktøj" i form af de to informationsnormer, der hviler den forståelse, at enhver forandring i praksis vil give anledning til "rødt lys" (Nissenbaum, 2010, s. 159-160). Derfor er det væsentligt at anvende de kontekstuelle informationsnormer hensigtsmæssigt. Enhver handling, som på den ene eller anden led overskri-

der eksisterende informationsnormer i en kontekst, skal undersøges nærmere. Men de skal ikke afvises per automatik (Nissenbaum, 2010, s. 159-160).

Kontekstuel integritet er en konservativ grundtanke, der er skeptisk overfor forandringer. Dette er problematisk, ikke mindst fordi *kontekstuel integritet* primært er rettet imod socio-tekniske systemer, hvor udviklingen er massiv. Hvis man ikke er åben overfor forandringer, kan dette være på bekostning af betydningsfulde udviklingsmuligheder. Omvendt kan det være problematisk, hvis man omfavner muligheder, hver gang de tilbydes, uden at reflektere over, hvad konsekvensen er.

I forlængelse af ovenstående opstår et andet problem ved brug af *kontekstuel integritet* og de to informationsnormer. Hvorledes sikres det, at man ikke tillader, at "for meget" ændrer sig? (Nissenbaum, 2010, s. 160-161). Blot fordi nuværende normer foreskriver en bestemt praksis, så behøver det ikke følge deraf, at den fremadrettede praksis skal følge samme spor. Eksempler kan være kameraovervågning af gader og stræder i London, som også tidligere er nævnt. I dag er den form for overvågning blevet accepteret, og det er dermed svært at gøre indsigelse (Nissenbaum, 2010, s. 161).

En mulig løsning er, at man ikke antager, at kompromittering af en eller begge informationsnormer nødvendigvis er problematisk, men blot forholder sig til, at der nu er en *prima facie*-forandring i forhold til eksisterende normer. For at opretholde sin moralske autoritet må *kontekstuel integritet* dog "kunne noget mere" end blot at påpege forandringer (Nissenbaum, 2010, s. 165-166).

En løsningsmodel kan bestå i, at man sammenligner den eksisterende normative praksis med den nye praksis med henblik på at evaluere, hvor effektive disse forskellige praksisser er til at opnå kontekstuelle værdier (Nissenbaum, 2010, s. 166). Med hensyn til en sikkerhedsteknologi kan man eksempelvis undersøge, i hvilken grad man mener, at et system vil effektivisere arbejdsgange og nedsætte antallet af bestemte forbrydelser. Denne sammenligning skal dog ske under hensynstagen til relevante værdier. Det er dermed ikke nok blot at undersøge, om en given kriminalitetsform nedsættes (Nissenbaum, 2010, s. 166).

I det tilfælde, hvor en ny praksis er mere effektiv og hensigtsmæssig, er det tilladeligt indenfor rammerne af *kontekstuel integritet* at "udskifte" den gamle praksis med den nye. Såfremt det ikke er tilfældet, må man undlade dette (Nissenbaum, 2010, s. 166).

4.3. PRIVATHED SOM ET FÆLLES GODE

Der findes en række perspektiver, der belyser privathed som en værdi for stat og samfund (Gavison, 1984; Peissl, 2003; Regan, 1995; Reiman, 1995; Solove, 2007).

Gavison (1984) påpeger blandt andet, at privathed har værdi for samfundet, idet privathed er essentiel for demokratiets levedygtighed (Gavison, 1984, s. 369). Solove (2007) understreger, at et samfund uden privathed ville være en kvælende oplevelse for et individ og ikke et sted, man har lyst til at leve. Hvis samfundet "holder sig tilbage" og lader individet opleve frihedszoner, så er der ifølge Solove mulighed for, at individet kan blomstre (Solove, 2007, s. 762). Man kan tale om respekt for individet og individets integritet. Ydermere har Solove påpeget, at overvågning kan få konsekvenser for et samfund som helhed, og at personer vil blive ensrettede med nedsat mulighed for at deltage i politiske aktiviteter (Solove, 2007, s. 765).

Regan (1995), der har et veludviklet, teoretisk syn på privathed som værdi for samfundet, opererer med tre forskellige værdier, der tilsammen begrunder, hvorfor privathed er væsentlig : *En fælles værdi*[90], *en offentlig værdi*[91] og *en kollektiv værdi*[92] (Regan, 1995, s. 213). Jeg vender tilbage til en udredning af Regans begrebsapparat i afsnit, 4.3.2., *Privathed: Relationen mellem stat og individ.*

Det er en antagelse i afhandlingen, at privathed ikke kun er værdifuld for det enkelte individ. At tillade privathed kommer også staten og samfundet til go-

[90] Egen oversættelse af "a common value" (Regan, 1995, s. 213).

[91] Egen oversættelse af "a public value" (Regan, 1995, s. 213).

[92] Egen oversættelse af "a collective value" (Regan, 1995, s. 213).

de. Det er netop formålet med nærværende afsnit at vise, at denne påstand er korrekt.

Når vi behandler et emne som privathed, så behandler vi også implicit, hvilket samfund vi ønsker. Opfattelsen, at privathed er væsentligt for stat og samfund, må nødvendigvis også indebære, at staten har en vis ontologisk selvstændighed. Har man et absolutistisk syn på relationen mellem stat og individ som eksempelvis Thomas Hobbes (2001), vil implikationen af en sådan ontologisk relation mellem stat og individ være, at individer er uden eller med kun ringe ret til privathed. Synspunktet, at privathed kan spille en rolle i forhold til staten, forudsætter trods alt, at statens eksistens anerkendes. Diskussionen af den ontologiske relation mellem stat og borger vender jeg tilbage til i kapitel 6., *Offentlig sikkerhed.*

4.3.1. PRIVATHED: EN BETINGELSE FOR DET LIBERALE DEMOKRATI

I dette afsnit vil jeg diskutere privathed som en nødvendig betingelse for demokratiet (Gavison, 1984; Peissl, 2003; Reiman, 1995) og redegøre for, hvordan privathed kan påvirke demokratiet på to forskellige måder.

For det første hviler et demokrati på, at individer tør træffe egne beslutninger og tænke egne tanker (Gavison, 1984, s. 369). Udviklingen af autonome individer er betingelsen for det velfungerende demokrati (Gavison, 1984, s. 369; Peissl, 2003, s. 22). Såfremt man godtager dette synspunkt, så bliver privathed særdeles vigtig – ikke kun for den enkeltes velbefindende, men som et grundlæggende fundament for den demokratiske stat og samfundets virke.

Reiman har også påpeget relationen mellem den liberale ide og privathed og disse to værdiers rolle i forhold til demokratiet (Reiman, 1995, s. 42). Den liberale ide bygger på det autonome individ. Det autonome individ har brug for et privathed. For at kunne opretholde relationerne mellem autonomi og privathed til fordel for demokratiet må staten tillade, at individer har mulighed for privathed. Tillader staten ikke, at individer kan udvikle egne perspektiver, bliver: "[...] democratic voting becomes mere ratification of conventionality, and individual freedom mere voluntary conformity." (Reiman, 1995, s.

42). Privathed er således en betingelse for demokratiet og dermed for opretholdelse af noget, som man i hvert tilfælde i den vestlige verden værdsætter.

Gavison har endvidere påpeget, at det er ønskværdigt at have et samfund, hvor individets autonomi, menneskelige relationer og muligheden for at leve et meningsfuldt liv ydes gode betingelser, hvilket leder til et pluralistisk, tolerant samfund (Gavison, 1984, s. 369). Gavisons argumentation kan rubriceres som utilitaristisk, idet individets opretholdelse af privatheden kan anses for et gode for de mange.

Konsekvensen af at opfatte privathed som en nødvendig betingelse for et velfungerende demokrati har den betydning, at såfremt det enkelte individ skulle miste interessen for privathed, så er det stadig en nødvendig forudsætning for demokratiets virke og dermed i flertallets interesse.

Den begrundelse, mener jeg, betyder også, at der nu er et stærkt argument for at tillægge privathed stor betydning. Opretholdelse af privathed handler således ikke blot om den enkeltes personlige interesser. Opretholdelsen af privathed handler i bund og grund også om samfundet som helhed (Regan, 1995, s. 221).

Der kan yderligere argumenteres for, at privathed er en betingelse for, at forskellige politiske processer kan opretholdes. Privathed faciliterer, at de enkelte politiske partier kan skabe og forme deres politik uforstyrret (Gavison, 1984, s. 369-370). Ydermere sikrer privathed, at politiske partier kan indgå i diskussioner med andre partier om politiske emner – alt dette uden offentlighedens kendskab til de konkrete diskussioner. Ophævede man muligheden for privathed, ville begge disse politiske processer have særligt vanskelige levevilkår (Gavison, 1984, s. 369-370).

I forlængelse af ovenstående kan man gøre gældende, at privathed spiller en central rolle ved selve valghandlingen. Det er med andre ord ikke kun forud for et valg, at privathed er relevant. Helt konkret foregår selve valghandlingen som en fysisk afskærmet aktivitet, hvorved privathed sikres. Et valg, hvor væl-

gernes anonymitet ikke er garanteret, anerkendes i den vestlige verden slet ikke som demokratisk.

4.3.2. PRIVATHED: RELATIONEN MELLEM STAT OG INDIVID

Når privathed og sikkerhed skal balanceres i forhold til hinanden, bliver privathed anset for en instrumentel værdi, der knytter sig til individet. Dette er i modsætning til sikkerhed, der har værdi for både staten og samfundet (Regan, 1995, s. 213). Der er således tale om, at et statsligt organ overvåger individer.

De privathedsproblemer, der behandles i afhandlingen, opstår i relationen mellem staten og individet. Dermed er det også nødvendigt at belyse privathed med netop denne relation i mente. Det betyder imidlertid ikke, at forudgående diskussioner af overvågningens konsekvenser for individet ikke er relevante. De illustrerer blot, hvilke intrinsiske goder privathed kan lede til for individet. I dette afsnit vil jeg dog stille mere skarpt på privathed i lyset af relationen mellem stat og individ.

Såfremt privathed kun anses for et gode for individet, så står privatheden langt fra lige så centralt og stærkt, når nye love skal formuleres (Regan, 1995, s. 212). Anskuelsen, at privathed alene handler om relationer imellem individer, ses ofte i den filosofiske litteratur, men ifølge Regan omfatter privathed også forholdet imellem individer og samfundet. Værdien af privathed kommer således også til at handle om individets mulighed for at trække sig tilbage fra samfundet (Regan, 1995, s. 217). Kan man derimod *også* forankre privathed som et fælles gode, kan det være med til at styrke argumentet for opretholdelse privathed (Regan, 1995, s. 220). En afgørende fordel ved at etablere et argument for privathed, der ikke blot relaterer sig til individet, er også, at såfremt den enkelte mister interessen i privathed, så er det ikke en begrundelse for ikke at opretholde privathed – privathed har netop også en social værdi (Regan, 1995, s. 221).

Med henblik på at demonstrere privathedens værdi som et socialt gode har Regan introduceret tre begreber: Privathed som *fælles værdi*[93], privathed som

[93] Egen oversættelse af "a common value" (Regan, 1995, s. 213).

en offentlig værdi[94] og privathed som *en kollektiv værdi*[95]. Jeg vil redegøre for disse begreber i nedenstående og efterfølgende påpege, hvordan begreberne kan vise sig værdifulde med henblik på at understøtte den opfattelse, at privathed er et fælles gode.

Privathed som en fælles værdi betyder, at alle individer har en fælles interesse i privathed. Individer opfatter og udlever måske nok privathed forskelligt, men de har alle en interesse heri (Regan, 1995, s. 221). Privathed opfattes således som en universel værdi. Individer, der lever i et tolerant og socialt pluralistisk samfund, kan bidrage til samfundet – ikke kun fordi det er væsentligt for dem selv, men også fordi: "[...] differences are part of the fabric of society. Differences contribute to the whole, not just the individual parts." (Regan, 1995, s. 222).

Privathed som en offentlig værdi indebærer, at privathed er en instrumentel værdi i forhold til det demokratiske, politiske system (Regan, 1995, s. 225). Privathed er af afgørende betydning for ytringsfrihed og friheden til at blive associeret med de mennesker eller grupper, som man ønsker – rettigheder, der er anset for værende essentielle for demokratiets virke (Regan, 2002, s. 399). Ydermere påpeger Regan, at privathed er væsentlig for den liberale ide om en begrænset stat. Privathed kan således være med til at etablere en grænse mellem statsmagten og individet (Regan, 1995, s. 225). Med forståelse af privathed som en offentlig værdi betoner Regan værdien af privathed på samme måde som eksempelvis Gavison.

Privathed som en kollektiv værdi er et begreb, som Regan har hentet i den økonomiske teori om såkaldte offentlige eller fælles goder. For denne type af goder gælder det, at: "[...] no one member of society can enjoy the benefit of a collective good without others also benefiting." (Regan, 1995, s. 213). Ren luft er et sådant gode. Kollektive goder fremmes ikke effektivt af et marked, og når

[94] Egen oversættelse af "a public value" (Regan, 1995, s. 213).

[95] Egen oversættelse af "a collective value" (Regan, 1995, s. 213).

først et kollektivt gode er givet, kan man ikke fratage nogle at anvende dette. Desuden gælder det for denne type af goder, at de er gratis.

Grundlæggende argumenterer Regan således for en privathedsmodel, der lægger op til mere offentlig regulering. Regan påpeger, at privathed ofte bliver opfattet som et gode, der knytter sig til individet, og at det er op til det enkelte individ at etablere det ønskede niveau af privathed. Der er således tale om en individorienteret og markedsbaseret tilgang til privathed, hvor det er op til den enkelte at sikre sin privathed. Eksempelvis kan man sikre, at ens telefonnummer ikke bliver vist, når man ringer til andre. Eller man kan krydse af, at man ikke ønsker sine informationer videresolgt, når man opretter et abonnement på et magasin (Regan, 1995, s. 228).

Jeg deler Regans bekymring for følgerne af en individorienteret, markedsbaseret privathedsmodel, hvor det er op til den enkelte at sikre sin privathed. Samtidigt må det dog påpeges, at denne markedsbaserede tilgang til privathed, der i høj grad understøtter virksomheders udfoldelsesmuligheder og hviler på ideen om det frie marked, er langt mere udtalt i USA end i EU. I EU har man netop i kraft af det nuværende Databeskyttelsesdirektiv 95/46/EF valgt at beskytte individer igennem beskyttelse af data. I kapitel 5., *Databeskyttelse: Retskilder og etikkens berettigelse,* belyses europæisk databeskyttelseslovgivning i flere detaljer. I samme kapitel findes en sammenligning af europæisk og amerikansk databeskyttelseslovgivning.

Regan oplister tre årsager til, at en markedsbaseret privathedsmodel ikke er levedygtig: *Tredjepartsorganisationer, ikke frivillige relationer* og *computer- og kommunikationsteknologier* (Regan, 1995, s. 228).

Tredjepartsorganisationer har data om individer til rådighed. Disse data er i praksis organisationernes ejendom – ikke individets. Til trods for at man som individ i nogen grad kan vælge at få fjernet disse informationer eller i hvert fald få indsigt heri[96], så bemærker Regan også, at det sjældent sker. Personer

[96] I EU gør Databeskyttelsesdirektivet gældende, at man har ret til indsigt i egne personrelaterede ??data (Europa-parlamentet og rådets direktiv, 1995, art. 12).

ved ikke, hvordan de skal tilgå dette marked, og hvorledes markedet opererer (Regan, 1995, s. 228). Den markedsbaserede tilgang til privathed betyder, at virksomheder kan profitere af at have data til rådighed, hvilket er et incitament for at indsamle data (Regan, 1995, s. 228). Dette modarbejder individets mulighed for at opretholde privathed.

Der eksisterer *ikke en frivillig relation* mellem individet og den, der indsamler data om individet. Når stater indsamler individrelaterede data (eksempelvis i forbindelse med skat), så kan man som individ ikke vælge, at man ikke ønsker sådanne informationer indsamlet (Regan, 1995, s. 229). Private virksomheder som fx banker indsamler ligeledes informationer. Her kan man som individ vælge en anden bank eller ikke at have en bank. Særligt den sidste mulighed eksisterer dog ikke i praksis i dag (Regan, 1995, s. 229). Dette hæmmer ligeledes muligheden for at opretholde privathed. Man må også overveje, om det ikke er nytteløst, hvad beskyttelse af ens privathed angår, at skifte bank.

Computer- og kommunikationsteknologier betyder, at data er let tilgængelige, og sammenhængen mellem systemer betyder, at data kan udveksles herimellem. Når computer- og kommunikationsteknologier er etablerede, bliver det nærmest umuligt for det enkelte individ at skabe sit eget ønskværdige niveau af privathed (Regan, 1995, s. 229-330).

Der er nu præsenteret en række grunde til, at det er problematisk at lade markedskræfter være styrende for privathed. Ydermere betoner Regan væsentligheden af, at der består et gensidigt afhængighedsforhold mellem den institutionelle part og individet. Såfremt et stort antal individer ikke ønskede at have en bankkonto, ville det have omfattende følger for et samfund og være ineffektivt for såvel bank som samfund (Regan, 1995, s. 229-330). Regans formål med at fundere privathed som en værdi, der ikke kun er værdifuld for individer, er, at dette kan have en række positive konsekvenser for, hvordan det er rimeligt at udvikle politik om privathed (Regan, 1995, s. 231). Konkret i forhold til informationel privathed kan Regans forståelse medføre, at privathed ikke opfattes som individets kontrol med information – eller muligheden for at kunne have kontrol med information. Derimod vil privathed blive:

"[...] defined as a right of a society to require institutions using personal information to do so in a manner that respects the shared interest in that information." (Regan, 1995, s. 232). Regans argumentation tager afsæt i en amerikansk kontekst, og derfor kan man godt argumentere for, at den tilgang, som hun efterlyser, i højere grad er til stede i EU end i amerikansk lovgivning. Regan anbefaler også selv, at man skeler til blandt andet EU i forsøget på at opnå beskyttelse af privathed, så det ikke kun er et individuelt anliggende (Regan, 1995, s. 234). Til trods for at blandt andre EU fremhæves af Regan som et forbillede i databeskyttelsessammenhænge, så vurderer jeg, at der er "mere at komme efter" i en europæisk sammenhæng. Jeg diskuterer og problematiserer retskilder om databeskyttelse i afhandlingens næste kapitel.

Forankringen af privathed som en social værdi betyder også, at man kan bevæge sig væk fra privathed som *den skyldige persons privilegium* (Regan, 1995, s. 234). At opfatte privathed udelukkende som en mulighed for at skjule ulovligheder er for snævert. Privathed spiller, som allerede demonstreret, en væsentlig instrumentel rolle for at opretholde intrinsiske goder.

I forlængelse af privathed som den skyldige persons privilegium vil jeg nu diskutere privathed i lyset af argumentet om, at hvis man ikke har noget at skjule, så har man heller ikke noget at frygte, når stater overvåger borgere.

4.4. PRIVATHED – "INTET AT SKJULE"-ARGUMENTET?

I dette afsnit vil jeg behandle et argument for overvågning, der jævnligt optræder i den offentlige debat om staters overvågning af borgere. Argumentet lyder, at såfremt man ikke har noget at skjule, så har man heller ikke noget at frygte i forhold til overvågning (Solove, 2007, s. 747). Argumentet bygger på en antagelse om, at privathed og sikkerhed er en dikotomi, og at fordelene ved at opretholde sikkerhed overstiger værdien af privathed.

Dette argument har jeg valgt at behandle, da det illustrerer et centralt element i afhandlingen. Når man vil balancere privathed i forhold til sikkerhed, så er udgangspunktet ofte, i hvilken grad overvågning vil skade individet, og i hvilken grad sikkerhed vil skabe samfundsmæssige fordele (Solove, 2007, s. 770).

Dette udgangspunkt hviler imidlertid på en snæver forståelse af privathed. I kraft af afhandlingens pluralistiske tilgang til privathed kan denne problemstilling og " intet at skjule"-argumentet problematiseres.

Jeg vil i nedenstående argumentere for, at hvis en person ikke ønsker at fremlægge informationer, så følger det ikke deraf, at man nødvendigvis har noget at skjule. Såfremt dette var tilfældet, ville det også kræve en forståelse af privathed, der primært havde hemmeligholdelse af information eller handlinger som fokus. Det er ikke tilfældet i afhandlingen. Værdien af privathed, der rækker videre end ønsket om at skjule information, er allerede fremlagt.

Et eksempel på et modargument til "intet at skjule"-påstanden optræder i følgende citat fra et debatindlæg på Politiken.dk:

> "Folk, der ønsker mere overvågning, argumenterer normalt med, at man ikke har noget at frygte, hvis man ikke har noget at skjule. Folk, der argumenterer sådan, burde gå foran og opstille et kamera i deres soveværelse.
>
> Vi har alle noget at skjule. Ikke nødvendigvis noget ulovligt. Men vores privatliv skal ikke invaderes af staten. Hvis man ikke har noget at skjule, hvorfor skal man så straffes med at blive overvåget?" (Jarlov, 2015).

Ovenstående og lignende modargumenter er ifølge Solove problematiske (Solove, 2007, s. 751). Solove påpeger, at:

> "Retorts to the nothing to hide argument about exposing people's naked bodies to the world or revealing their deepest secrets to their friends are only relevant if there is a likelihood that such programs will actually result in these kinds of disclosures. **This type of information is not likely to be captured in the government surveillance**." (min fremhævelse) (Solove, 2007, s. 752).

Ved første øjekast kan man måske være tilbøjelig til at give Solove ret. Det forekommer ikke at være sandsynligt, at statslige organer begynder at overvåge individer i deres soveværelse. På den anden sige kan man stille spørgsmålstegn ved, om argumentet nu virkelig er så svagt, da det *allerede* har været tilfældet, at staters systematiske overvågning af borgere kan have implikationer, der rækker helt ind i soveværelset. Her tænker jeg på sikkerhedstjenesten Stasis overvågning i det tidligere DDR. Således eksisterer der eksempler på, at

staters overvågning kan få betydning for forhold, der ofte udspiller sig i hjemmet.

Problemet med "intet at skjule"-argumentet er, at dette implicerer, at man behandler privathedstabets skade på individet i forhold til den mulige sikkerhedsfordel, som overvågning medfører for samfundet. Implicit i "intet at skjule"-argumentet ligger også en opfattelse af, at privathed ikke er lige så værdifuldt som sikkerhed – der er ikke tale om information, som er særlig væsentlig. Med mindre man har noget at skjule, selvfølgelig.

Det dybereliggende problem med "intet at skjule"-argumentet er den grundlæggende antagelse, som dette argument hviler på. Præmissen er, at privathed handler om *at skjule noget* (Solove, 2007, s. 765). Der er i afhandlingen netop argumenteret for, at privathed handler om en lang række af andre forhold end at kamuflere ulovligheder. Det er klart, at privathed *kan* være et skalkeskjul for ulovligheder, men jeg skønner, at det kun er relativt få individer, der nyder denne beskyttelse.

Et andet problem med omtalte argument er, at man måske nok kan udpege informationer, der som enkeltstående informationer ikke er problematiske. Men idet disse informationer sammenkøres, kan der måske afsløres forhold om et individ, som man alligevel ikke havde forventet (Solove, 2007, s. 766). Tidligere i afhandlingen er fremhævet et studie, der viste, hvordan man på baggrund af blandt andet "likes" fra Facebook kunne udlede forhold om personers seksuelle orientering, religiøse overbevisning og etnicitet (Kosinski, Stillwell, & Greapel, 2013). Dette studie kan også her anvendes som illustration af, at det kan være svært som individ at forudsige, hvad data kan bruges til, og ikke mindst hvad disse data kan forudsige.

Det er allerede diskuteret, at et problem med datamining er den mangelfulde transparens, der omgærder dette område. Denne problemstilling er også relevant i forhold til argumentet om ikke at have noget at skjule. De personer, der påpeger, at de ikke har noget imod overvågning, fordi de har intet at skjule, kan grundet avancerede datamining-teknikker ikke vide, hvad der konkluderes om dem på baggrund af indsamlede data (Solove, 2007, s. 766). På samme

måde kan datamining vise sig problematisk i forhold til social sortering og profiling, hvilket jeg også tidligere har omtalt. Blot fordi man ikke har noget at skjule, kan man godt ende i en kasse, som man måske ikke har lyst til at være i, og som måske kan få betydning for de muligheder, man har i livet (Solove, 2007, s. 766).[97]

Anerkendes argumentationen for, at privathed er et fælles samfundsgode, så bliver "intet at skjule"-argumentet uinteressant i den forstand, at privathed ikke kun har værdi for individet, men også for samfundet som hele. Det er dermed ikke længere blot et spørgsmål det enkelte individ overfor staten og en balancering af flertallets interesser overfor individets interesser.

"Intet at skjule"-argumentet beror på en antagelse om, at privathed er et gode for individet, mens sikkerhed er et gode for samfundet. Jeg har i nærværende afhandling udfordret denne opfattelse. Diskussion af udvalgte teoretiske perspektiver har demonstreret, at mangel på privathed som følge af staters overvågning af borgere kan have en række uhensigtsmæssige konsekvenser. Overvågning er således ikke kun problematisk for personer, der går med planer om at udføre terror eller om at drive forretning som menneskesmugler.

Privathed er behandlet som et gode for såvel stat og samfund som for individ. For individet er privathed en instrumentel værdi, idet privathed er en betingelse for en række særligt vigtige, intrinsiske goder som autonomi, integritet, intimitet og sociale relationer. Ydermere er det demonstreret, hvordan privathed er en betingelse for det liberale demokratis levedygtighed. Fratages individet privathed, så er det ikke blot individets tab.

Privathed har i aktuelle kapitel været belyst fra et filosofisk ståsted. Det er også relevant at anskue privathed i lyset af de retskilder, der anvendes til regulering af individers privathed – såkaldt databeskyttelse. Dette emne vil jeg redegøre for i kapitel 5., *Databeskyttelse: Retskilder og etikkens berettigelse.*

[97] Endnu et problem i forhold til omtalte argument er, at ens data, når de er indsamlet, kan anvendes til andre formål, end det oprindeligt er tiltænkt. Denne problematik påpeges andetsteds i afhandlingen, og jeg vil derfor ikke diskutere denne yderligere her.

5. DATABESKYTTELSE: RETSKILDER OG ETIKKENS BERETTIGELSE

5. DATABESKYTTELSE: RETSKILDER OG ETIKKENS BERETTIGELSE

I nærværende kapitels første afsnit, 5.1., *Retskilder vedrørende databeskyttelse i Den Europæiske Union*, vil jeg introducere en række relevante retskilder, som er gældende på nuværende tidspunkt, eller som har dannet grundlag for gældende ret på databeskyttelsesområdet. Dertil kommer, at den eksisterende databeskyttelseslovgivning i EU ikke længere anses som værende tidssvarende. En ny forordning er derfor under udarbejdelse. I kapitlets afsnit 5.1.6., *Ny databeskyttelsesforordning i EU*, omtales denne forordning.

I kapitlets afsnit 5.1.7., *EU og USA: Sammenligning af retskilder* vil jeg på et overordnet niveau påpege, hvor betydningsfulde forskelle, der eksisterer mellem europæiske og amerikanske retskilder vedrørende databeskyttelse og privathed. Reguleringen af databeskyttelse og privathed i EU og USA sammenlignes ofte, hvorfor det er relevant at illustrere sådanne forskelle. Denne sammenligning er også interessant, fordi lovgivningen i EU og USA bygger på samme grundlag, men er udformet og udfoldes særdeles forskelligt. Hertil kommer, at der findes en lang række af virksomheder, som er hjemmehørende i USA og er amerikansk ejede, og som har stor betydning for europæiske borgere – eksempelvis Google, Apple, Microsoft, Twitter og Skype. Derfor har amerikansk privathedsbeskyttelse, herunder det retlige samarbejde mellem USA og EU inden for dette område, stor betydning for EU-borgere. Det er klart, at privathed og databeskyttelse også er reguleret uden for hhv. EU og USA. Denne afhandling er imidlertid ikke et juridisk funderet projekt, hvis formål er at analysere gældende ret. Det er derfor kun den amerikanske lovgivning, der inddrages.

I kapitlets afsnit 5.2., *Etikkens berettigelse og ansvarlig udvikling af teknologi*, vil jeg behandle forholdet mellem etikken og de juridiske regler på databeskyttelsesområdet. Jeg vil begrunde, hvorfor etik stadig har en berettigelse ved siden af de juridiske regler på databeskyttelsesområdet, til trods for at der eksisterer en omfattende juridisk ramme på dette område. Endvidere vil jeg

diskutere, hvorfor den etiske dimension i forhold til udvikling af ny sikkerhedsteknologi stadig er betydningsfuld set i lyset af privathed. I denne forbindelse omtales såkaldt *Responsible research and innovation*, som er blevet et fokusområde i EU.

Det bemærkes, at når privathed omtales som *en ret* eller *en rettighed* i afhandlingen, så er der tale om en værdi, der giver sig udslag i en ret eller rettighed.

5.1. RETSKILDER VEDRØRENDE DATABESKYTTELSE I DEN EUROPÆISKE UNION

I afsnittene 5.1.1., *FN's menneskerettigheder og Menneskerettighedskonventionen* – 5.1.5., *Direktiv 95/46/EF og 2002/58/EF,* gives et overblik over relevante retskilder i relation til databeskyttelse, som er gældende på nuværende tidspunkt i EU. Derudover introduceres retskilder, der ikke længere er gældende, men som har haft væsentlig betydning for udviklingen af gældende ret. Retskilderne belyses i forhold til sikkerhed for nation og individ.[98] Som det er demonstreret tidligere i denne afhandling, har de data, der er tilgængelige om individet, betydningsfulde implikationer for dettes muligheder i livet. Dermed bliver måden, hvorpå data bliver beskyttet rent juridisk signifikant betydning. Ydermere introduceres den nye EU-forordning omhandlende databeskyttelse. Slutteligt sammenlignes lovgivning i EU og USA i afsnit 5.1.7., *EU og USA: Sammenligning af retskilder*.

5.1.1. FN'S MENNESKERETTIGHEDER OG MENNESKERETTIGHEDSKONVENTIONEN

Retten til beskyttelse af en privatsfære blev for første gang taget i betragtning af en international juridisk instans, da de Forenede Nationer[99] (herefter blot FN) i 1948 forfattede art. 12 i FN's Verdenserklæring om Menneskerettighe-

[98] Sikkerhedsbegrebet belyses ligeledes i forhold til en række retskilder i kapitel 6, *Offentlig sikkerhed*, afsnit 6.2., *Sikkerhedsbegrebet i udvalgte retskilder.*

[99] Formålet med FN er at sikre, at der opretholdes fred mellem medlemsstaterne. Derudover ønskes det også at sikre borgernes basale menneskelige rettigheder.

derne (De Forenede Nationer, 1948). Formålet hermed var en beskyttelse af det enkelte individ. Af art. 12 fremgår, at:

> "Ingen må være genstand for vilkårlig indblanding i private forhold, familie, hjem eller korrespondance, ej heller for angreb på ære og omdømme. Enhver har ret til lovens beskyttelse mod sådan indblanding eller angreb." (De Forenede Nationer, 1948, s. 12)

FN's Verdenserklæring fik indflydelse på Konvention til Beskyttelse af Menneskerettigheder og Grundlæggende Frihedsrettigheder[100], der blev udfærdiget i Rom i 1950, og som trådte i kraft i 1953[101]. Menneskerettighedskonventionen er en juridisk bindende traktat (Raguse, 2008, s. 11).

Konventionens art. 8 udgør det juridiske grundlag for databeskyttelse i EU, og heri anerkendes retten til privatliv. Art. 8 lyder som følger:

> "Stk. 1. Enhver har ret til respekt for sit privatliv og familieliv, sit hjem og sin korrespondance.
>
> Stk. 2. Ingen offentlig myndighed kan gøre indgreb i udøvelsen af denne ret, undtagen forsåvidt det sker i overensstemmelse med loven og er nødvendigt i et demokratisk samfund af hensyn til den nationale sikkerhed, den offentlige tryghed eller landets økonomiske velfærd, for at forebygge uro eller forbrydelse, for at beskytte sundheden eller sædeligheden eller for at beskytte andres ret og frihed." (Folketingets EU-oplysning).

Som det fremgår af artiklens ordlyd, indeholder dennes stk. 1 hovedreglen, mens stk. 2 indeholder en undtagelse dertil. Således gøres det i stk. 1 klart, at: "Enhver har ret til respekt for sit privatliv og familieliv, sit hjem og sin korrespondance.". Menneskerettighedskonventionens begreb "respekt for privatliv" skal forstås bredt og med særligt sigte på at lade det enkelte individ have relationer til andre mennesker (Kjølbro, 2005, s. 433). En præcis fortolkning af begrebet "respekt for privatliv" kan ifølge landsdommer Jon Fridrik Kjølbro ikke gives, men dette retskrav kan dække over "[...] en persons fysiske og psy-

[100] Det er den Europæiske Menneskerettighedsdomstol i Strasbourg, der behandler sager om overtrædelse af konventionen.

[101] I Danmark blev Menneskerettighedskonventionen først formelt en del af dansk lovgivning i 1992.

kiske integritet." (Kjølbro, 2005, s. 433) og "[...] en persons fysiske og sociale identitet" (Kjølbro, 2005, s. 433).[102] Disse måder at anskue privathed på findes der paralleller til i de filosofiske begrundelser, der er givet for privathed (se eksempelvis Fried, 1984; Rachels, 1984; Reiman, 1984).

Art. 8, stk. 2, udgør som nævnt en undtagelse til hovedreglen og fastsætter, at offentlige myndigheders indgreb i retten til privathed kan tillades, hvor visse nærmere beskrevne betingelser er opfyldt. Således er det i stk. 2 gjort klart, at man anerkender, at der er et samfundsmæssigt hensyn at varetage i forhold til individets ret til privathed. Jeg vil nedenfor kort beskrive to af disse betingelser, nærmere at indgreb i retten til privatliv m.v. skal 1) "[...] være i overensstemmelse med loven [...] og 2) "[...] nødvendigt i et demokratisk samfund[...]".

Art. 8, stk. 2 fastsætter som den første betingelse, at indgreb i retten til privatliv m.v. skal "[...] være i overensstemmelse med loven [...]". Dette betyder, at der skal være hjemmel i den nationale ret i forhold til de oplistede formål[103], hvilket er en refleks af det såkaldte legalitetsprincip. Legalitetsprincippet indebærer ydermere, at lovgivningen skal være rimeligt forudsigelig og offentliggjort. Det vil med andre ord sige, at det skal være synligt og forståeligt for borgeren, hvorledes der reguleres.

I art. 8, stk. 2, anføres som den anden betingelse, at indgrebet skal være: "[...] nødvendigt i et demokratisk samfund[...]". Nødvendigt skal her forstås som et

[102] De Hert (2005) har dog stillet spørgsmålstegn ved, om Menneskerettighedsdomstolen i tilstrækkelig grad lader art. 8, stk 1, i Menneskerettighedskonventionen indfange bløde (teknologiske) overvågningsmidler (De Hert, 2005, s. 88-92), og påpeger i den forbindelse at: "The Strasbourg institutions seem to find more and more difficulty in recognizing the fundamental nature of privacy and the plain fact that it does not require blood (but technology) to violate it." (De Hert, 2005, s. 89). Såfremt kritikken er berettiget, forekommer en sådan praksis problematisk, eftersom bløde, måske privathedskompromitterende overvågningsteknologier i særdeleshed vinder frem.

[103] Dette kan blandt andet ses i afgørelsen fra Menneskerettighedsdomstolen i sagen Leander v. Sweden (application no. 9248/81), 26 March 1987, hvor der i paragraf 50 er anført, at: "The expression "in accordance with the law" in paragraph 2 of Article 8 (art. 8-2) requires, to begin with, that the interference must have some basis in domestic law. Compliance with domestic law, however, does not suffice: the law in question must be accessible to the individual concerned and its consequences for him must also be foreseeable [...]".

pressing social need[104]. For at dette kan opretholdes, skal tre forskellige forhold, der kan udledes af retspraksis fra Den Europæiske Menneskerettighedsdomstol, tages i betragtning (van Loenen, Groetelaers, Zevenbergen, & de Jong, 2007, s. 142).

For det første kræves at: "[...] a fair balance has to be struck between the demands of the general interest and the interest of the individual." (van Loenen, Groetelaers, Zevenbergen, & de Jong, 2007, s. 142). For det andet skal "nødvendighedsbetingelsen" ses i lyset af proportionalitetsprincippet, der er et væsentligt princip inden for offentlig ret. I EU-retten indebærer proportionalitetsprincippet, at lovgiver skal handle i det omfang, der er nødvendigt i forhold til at opnå EU-traktatens[105] mål (Proportionalitetsprincippet).[106] Disse mål er blandt andet at fremme økonomiske og sociale fremskridt, iværksætte en fælles udenrigs- og sikkerhedspolitik og på sigt skabe et fælles forsvar og styrke beskyttelsen af medlemsstaternes statsborgeres rettigheder ved at skabe et unionsborgerskab (Generalsekretariatet for Rådet og Kommisionen, 1992, art. b). For det tredje nævnes det, at: "[...] interference can only be regarded as 'necessary in a democratic society' if the particular system of secret

[104] Begrebet er ikke oversat, da der ikke findes en passende dansk betegnelse.

[105] EU-traktaten, der henvises til, kaldes også Maastricht –traktaten, hvori der blandt andet er bestemmelser om demokratiske principper, samarbejde, sikkerhed og udenrigspolitiske spørgsmål.

[106] Dette kan blandt andet ses i afgørelsen på Klass and Others v. Germany, (application no. 5029/71), 6 September 1978 i dele af paragraf 48 og 49, hvori det er anført, at: "Democratic societies nowadays find themselves threatened by highly sophisticated forms of espionage and by terrorism, with the result that the State must be able, in order effectively to counter such threats, to undertake the secret surveillance of subversive elements operating within its jurisdiction. The Court has therefore to accept that the existence of some legislation granting powers of secret surveillance over the mail, post and telecommunications is, under exceptional conditions, necessary in a democratic society in the interests of national security and/or for the prevention of disorder or crime. [...] Nevertheless, the Court stresses that this does not mean that the Contracting States enjoy an unlimited discretion to subject persons within their jurisdiction to secret surveillance. The Court, being aware of the danger such a law poses of undermining or even destroying democracy on the ground of defending it, affirms that the Contracting States may not, in the name of the struggle against espionage and terrorism, adopt whatever measures they deem appropriate.".

surveillance adopted contains adequate guarantees against abuse." (van Loenen, Groetelaers, Zevenbergen, & de Jong, 2007, s. 143).

Grundlaget for ovenstående er, at det offentlige apparat (indenfor såvel EU som på nationalt plan) principielt har en udstrakt adgang til at misbruge skjult overvågning overfor det enkelte individ. Et sådant misbrug ville have betydelige konsekvenser for et demokratisk samfund (van Loenen, Groetelaers, Zevenbergen, & de Jong, 2007, s. 143).

Art. 8 udpeger således ikke en absolut ret til privathed, men en rettighed, der skal balanceres i lyset af andre forhold – eksempelvis national sikkerhed. I det næste kapitel 6, *Offentlig sikkerhed* omhandlende værdien offentlig sikkerhed eksemplificeres det, hvad konsekvensen af denne ikke absolutte ret til privathed kan betyde. Dette sker ved omtale af en konkret dom[107] fra Menneskerettighedsdomstolen i Strasbourg.

5.1.1.1. PROPORTIONALITETSPRINCIPPET I EU-RET

I det følgende vil jeg kort diskutere udvalgte problematikker forbundet med overholdelsen af det ovenfor omtalte proportionalitetsprincip. Jeg vil i forbindelse hermed anføre konkrete eksempler.

I forhold til f.eks. *dataveillance* kan proportionalitetsprincippet vise sig problematisk at overholde. Et konkret eksempel herpå er datamining, der kan anvendes som en præventiv metode eksempelvis i forhold til kriminalitet. Datamining, der er en kombination af dataanalyse og brug af avancerede algoritmer, er et led i en mere omfattende proces: *knowlegde discovery*[108]. Formålet med *knowlegde discovery* er at transformere rå data til brugbar information (Monreale, 2011, s. 27).

Datamining kan bruges til at finde ukendte mønstre eller strukturer indeholdt i databaser. *Datamining* er derved karakteriseret ved, at man ikke ved, hvad

[107] Leander v. Sweden (application no. 9248/81), 26 March 1987.

[108] Begrebet er ikke oversat, da der ikke findes en passende dansk betegnelse.

man vil finde ud af, når man miner data – i modsætning til traditionelle udtræk fra databaser, hvor man *spørger*[109] om noget bestemt[110].

Datamining-opgaver falder i to kategorier: *Beskrivende*[111] og *prædiktiv*[112]. Beskrivende datamining har til formål at præsentere de centrale træk i et datasæt. Prædiktiv datamining sigter derimod mod at opnå en forudsigelse om et bestemt forhold (Monreale, 2011).[113] I eksempelvis politiets arbejde kan *datamining* udføres før, der overhovedet er et kendskab til kriminelle handlinger – dvs. på et tidspunkt, hvor man ikke har specifikke mistænkte (Monreale, 2011; Raguse, 2008, s. 30). Det betyder også, at jo færre informationer man har om konkrete personer eller handlinger, desto mere har undersøgelsen karakter af "at lede efter en nål i en høstak" (Raguse, 2008, s. 30).

Der kan med rimelighed stilles spørgsmålstegn ved, om denne måde at masseovervåge individers data på, kolliderer med art. 6, stk. 2, i Menneskerettighedskonventionen. Art. 6[114] omhandler retten til en retfærdig rettergang, og af

[109] Egen oversættelse af "querying".

[110] Eksempelvis kan man foretage et udtræk fra en database, hvor man ønsker at se personer, der har fornavnet Dorte, er mere end 45 år gamle og bor i Vejle.

[111] Egen oversættelse af termen "descriptive" (Monreale, s. 27).

[112] Egen oversættelse af termen "predictive" (Monreale, s. 27).

[113] Datamining er en kompleks teknologi, som kunne beskrives væsentligt mere indgående end gjort her. Da afhandlingen er et it-etisk projekt, hvor forskellige teknologier og deres anvendelse er inddraget for at eksemplificere teoretiske pointer, har jeg valgt ikke at indføje en sådan mere dybdegående beskrivelse, idet dette ikke er skønnet nødvendigt eller hensigtsmæssigt.

[114] Menneskerettighedskonventionens art. 6 (Stk. 3 er udeladt):

"Stk. 1. Enhver skal, når der skal træffes afgørelse enten i en strid om hans borgerlige rettigheder og forpligtelser eller angående en mod ham rettet anklage for en forbrydelse, være berettiget til en retfærdig og offentlig rettergang inden en rimelig frist for en ved lov oprettet uafhængig og upartisk domstol. Dom skal afsiges i offentligt møde, men pressen og offentligheden kan udelukkes helt eller delvis fra retsforhandlingerne af hensyn til sædeligheden, den offentlige orden eller den nationale sikkerhed i et demokratisk samfund, når det kræves af hensynet til mindreårige eller til beskyttelse af parternes privatliv, eller under særlige omstændigheder i det efter rettens mening strengt nødvendig omfang, når offentlighed ville skade retfærdighedens interesser.

dennes stk. 2 følger, at: "Enhver, der anklages for en lovovertrædelse, skal anses for uskyldig, indtil hans skyld er bevist i overensstemmelse med loven." (Folketingets EU-oplysning, art. 6, stk. 2).

Spørgsmålet er nu, om indsamling af data vedrørende en hel befolkning eller en større gruppe af individer, der ikke er under konkret mistanke, må anses som værende i strid med art. 6, stk. 2. Er et individ virkelig anset for at være uskyldigt, hvis det alligevel synes nødvendigt at indsamle data om dette individ? Det er De Herts opfattelse, at individet først er beskyttet af art. 6, stk. 2, når dette ikke længere gør sig fortjent til prædikatet "uskyldig" (De Hert, 2005, s. 85). På den måde kan overvågningsmuligheder som *dataveillance* udfordre den nuværende lovgivning. I denne sammenhæng skal det dog nævnes, at Menneskerettighedskonventionen skal fortolkes dynamisk, og derved skal ses som: "[...] a living instrument which should be interpreted according to present-day conditions." (De Hert, 2005, s. 74).

En måde, hvorpå den problematik, som De Hert påpager, kan afhjælpes, kunne være, at politiet (eller den anden instans, der måtte forestå en efterforskning) nøjagtigt vurderer sagen i lyset af proportionalitetsprincippet og vælger den efterforskningsmetode, der er mest skånsom i forhold til det enkelte individ og dennes ret til privathed (Raguse, 2008, s. 30). Dette synes at være mest rimeligt i forhold til at give den enkeltes privathed bedre levevilkår. I proportionalitetsprincippet ligger videre, at en krænkelse af privathed skal være proportional med den forbedring af sikkerhed, som der derved opnås.

Logningsdirektivet, der er blevet kaldt det mest privacy-invaderende instrument i EU nogensinde (Institut for Menneskerettigheder, 2015, s. 13-14), var et tydeligt eksempel på, at indsamling af data om borgere, ikke var proportional med indsamlingens udbytte. Man indsamlede data om alle borgere til trods for, at det kun var et fåtal, der var mistænkte.

Stk. 2. Enhver, der anklages for en lovovertrædelse, skal anses for uskyldig, indtil hans skyld er bevist i overensstemmelse med loven." (Folketingets EU-oplysning, art. 6).

Staters masseovervågning og logning kan helt generelt problematiseres i lyset af proportionalitetsprincippet. Blot fordi et givent system til overvågning af data kan anvendes (eller konkret anvendes) med henblik på at øge den nationale sikkerhed, betyder det ikke, at systemet ikke kan komme i konflikt med proportionalitetsprincippet. Hvis en stat indsamler massive mængder data om en persongruppe – som man eksempelvis har gjort det for at leve op til Logningsdirektivet i Danmark – men det kun er data vedrørende en lille gruppe af de personer, der indsamles data om, der egentlig har interesse, kan dette sammenlignes med, at man leder efter en nål i en høstak. Selvom formålet er at øge sikkerhed for en nation, så er det for vidtgående at "indsamle hele høstakken" ifølge en resolution fra FN (Human Rights Council, United Nations, 2014, s. 8-9, §§ 24-25). At lede efter en nål i en høstak med det formål at øge sikkerheden kan således ikke udgøre et grundlag for at legitimere masseovervågning. Det egentlig mål for, hvorvidt en given overvågningsforanstaltning er i overensstemmelse med proportionalitetsprincippet, er overvågningsforanstaltningens indvirkning på hele høstakken i forhold til den potentielle skade, man afværger (Human Rights Council, United Nations, 2014, s. 8-9, §§ 24-25). I forhold til Logningsbekendtgørelsen i Danmark er dette problematisk, idet den indsamlede data ikke udgjorde nogen reel forskel for sikkerheden.

Bedømmelsen af en given sikkerhedsteknologis virkning kan også mere konkret problematiseres i forhold til proportionalitetsprincippet. Hvis man efter implementering af et givent system kan konstatere, at eksempelvis organiseret kriminalitet stagnerer, eller man ser en tilbagegang heri, følger det ikke nødvendigvis heraf, at det er den konkrete sikkerhedsteknologi, der er den udløsende årsag til forandringen. Antager man, at sikkerhedsteknologien ikke er årsag til forandringen, kan man stille spørgsmålstegn ved, hvorvidt anvendelsen af systemet er sket med respekt for proportionalitetsprincippet. En sådan overvejelse må henhøre under juridiske overvejelser, hvilket i falder uden for afhandlingens genstandsfelt.

Ydermere arbejdes der i EU-ret med såkaldt *margin of appreciation*[115], hvilket implicerer, at man kan: "[...] operate within certain boundaries provided by the European framework." (van Loenen, Groetelaers, Zevenbergen, & de Jong, 2007, s. 144). I praksis betyder det, at der tages hensyn til, at de enkelte medlemslande vil opfatte Menneskerettighedskonventionen forskelligt, og at de enkelte medlemslande dermed også kan bestemme, hvorledes de vil balancere sikkerhed og privathed i praksis.[116] van Loenen et al bemærker, at denne *margin of appreciation* blandt andet i Holland i højere grad er blevet brugt til at fremme nationale sikkerhedsinteresser efter terrorangrebet den 11. september, hvor panikken bredte sig, og beslutninger omkring lovgivning blev taget med afsæt i en ide om, at flere midler nødvendigvis er bedre (van Loenen, Groetelaers, Zevenbergen, & de Jong, 2007, s. 144, 150).

5.1.2. DEN EUROPÆISKE UNIONS CHARTER OM GRUNDLÆGGENDE RETTIGHEDER

I 1999 samlede Det Europæiske Råd[117] en række grundlæggende rettigheder i et charter. Dette er navngivet Den Europæiske Unions Charter om Grundlæggende Rettigheder (Den Europæiske Union, 2010). Formålet hermed var at øge synligheden af grundlæggende rettigheder i EU, og chartret beskriver detaljeret medlemslandenes forpligtigelser i forhold til EU's værdier[118]. Dele af

[115] Begrebet er ikke oversat, da der ikke findes en passende dansk betegnelse.

[116] Dette kan blandt andet ses i afgørelsen fra Menneskerettighedsdomstolen Leander v. Sweden (application no. 9248/81), 26 March 1987, hvor der i paragraf 59 står anført at: "[...] the Court recognises that the national authorities enjoy a margin of appreciation, the scope of which will depend not only on the nature of the legitimate aim pursued but also on the particular nature of the interference involved. In the instant case, the interest of the respondent State in protecting its national security must be balanced against the seriousness of the interference with the applicant's right to respect for his private life.".

[117] Det Europæiske Råd fastlægger de overordnede politiske retningslinjer og mål for den Europæiske Union, EU. Det Europæiske Råd blev oprettet i 1974 og fik formel status i 1992 i kraft af Maastrichttraktaten. I 2009 blev Det Europæiske Råd i kraft af Lissabontraktaten én af unionens 7 institutioner. Samtlige EU-medlemslande er medlemmer af Det Europæiske Råd, hvorfor disse også juridisk er bundet heraf (Raguse, 2008, s. 10).

[118] EU's værdier er anført i EU-traktaten: "[...] Unionen bygger på værdierne respekt for den menneskelige værdighed, frihed, demokrati, ligestilling, retsstaten og respekt for menneskerettighederne, herunder rettigheder for personer, der tilhører mindretal. Dette er medlemsstaternes fælles værdigrundlag i et samfund præget af pluralisme, ikke- forskelsbehandling, tolerance, retfærdighed, solidaritet og ligestilling mellem kvinder og mænd." (Den Europæiske Union, 2005)

chartrets bestemmelser er baseret på Menneskerettighedskonventionen. Såfremt dette charter indeholder rettigheder, der også er sikret ved Menneskerettighedskonventionen, har de af chartret omfattede rettigheder samme omfang og betydning som i Menneskerettighedskonventionen. (Den Europæiske Union, 2010, s. 406, art. 52, stk 3). Dette charter blev gjort juridisk bindende for medlemsstaterne i december 2009 i forbindelse med Lissabontraktaten[119] (Europæiske Union, 2010; European Union Agency for Fundamental Rights, 2013, s. 21).

Den Europæiske Unions Charter om Grundlæggende Rettigheder består af 54 artikler, der alle fastlægger konkrete rettigheder for borgere indenfor kategorierne værdighed, frihed, ligestilling, solidaritet, borgerrettigheder og retfærdighed i retssystemet. Heri gøres det blandt andet klart, at retten til respekt for privatliv og familieliv samt beskyttelse af personoplysninger er væsentlige rettigheder for borgere. Disse rettigheder er fæstet i chartrets art. 7 og 8, der findes i afsnittet om friheder (Europæiske Union, 2010, s. 397), og lyder som følger:

> "Artikel 7
>
> Respekt for privatliv og familieliv
>
> Enhver har ret til respekt for sit privatliv og familieliv, sit hjem og sin kommunikation.
>
> Artikel 8
>
> Beskyttelse af personoplysninger
>
> 1. Enhver har ret til beskyttelse af personoplysninger, der vedrører den pågældende.
>
> 2. Disse oplysninger skal behandles rimeligt, til udtrykkeligt angivne formål og på grundlag af de berørte personers samtykke eller på et andet berettiget ved lov fastsat grundlag. Enhver har ret til adgang til indsamlede oplysninger, der vedrører den pågældende, og til berigtigelse heraf.

[119] Dette charter er ikke en del af Lissabontraktaten, men der henvises i netop Lissabontraktaten til dette charter.

> 3. Overholdelsen af disse regler er underlagt en uafhængig myndigheds kontrol." (Den Europæiske Union, 2010, s. 397).

For såvel art. 7 som art. 8 i chartret gælder det, at bestemmelserne skal ses i lyset af stk. 1 i chartrets art. 52, der bærer overskriften Rækkevidde og fortolkning af rettigheder og principper. Af art. 52, stk. 1, fremgår det, at der kan: "[...] indføres begrænsninger, såfremt disse er nødvendige og faktisk svarer til mål af almen interesse, der er anerkendt af Unionen, eller et behov for beskyttelse af andres rettigheder og friheder." (Den Europæiske Union, 2010, art. 52). Begrænsningerne i rettigheder og principper skal ske under: "[...] iagttagelse af proportionalitetsprincippet [...]" (Den Europæiske Union, 2010, art. 52).

5.1.3. EUROPARÅDETS KONVENTION 108

Konvention om beskyttelse af det enkelte menneske i forbindelse med elektronisk databehandling af personoplysninger, også kaldet Konvention 108, er ratificeret af samtlige EU-medlemsstater og underskrevet den 28. januar[120] 1981. Formålet med Konvention 108 er at beskytte det enkelte individ mod misbrug i forbindelse med indsamling og behandling af personlige data (Lovbekendtgørelse nr. 59, af 16. maj 1991). Konvention 108 anses som en art forlængelse af Menneskerettighedskonventionen. Konvention 108 spiller en central rolle, da senere lovgivning på området bygger på de principper for databeskyttelse, der er anført i konventionens art. 5-9. Bestemmelserne lyder som følger:

> "Artikel 5
>
> Oplysningernes beskaffenhed
>
> Personoplysninger som behandles elektronisk skal:
>
> a. indsamles og behandles rimeligt og lovligt;
>
> b. lagres til nærmere bestemte og lovlige formål, og må ikke anvendes på en måde, som er uforenelig med disse formål;
>
> c. være relevante og tilstrækkelige, og ikke omfatte mere end, hvad der kræves til opfyldelsen af de formål, de er lagret til;

[120] Netop denne dag er også den Europæiske Databeskyttelsesdag.

d. være nøjagtige og, om nødvendigt føres ajour;

e. opbevares i en form, som ikke muliggør identifikation af de registrerede personer længere end nødvendigt til det formål, de er lagret til.

Artikel 6

Særlige typer af oplysninger

Personoplysninger vedrørende race, politisk overbevisning, religiøs eller anden trosbekendelse, såvel som personoplysninger om helbred og seksuelle forhold, må ikke behandles elektronisk, medmindre national gældende lovgivning yder fornøden beskyttelse. Det samme gælder personoplysninger vedrørende straffedomme.

Artikel 7

Sikkerhedsforanstaltninger

Elektroniske registre med personoplysninger skal sikres i fornødent omfang mod uagtsom eller uautoriseret ødelæggelse og tab ved uagtsomhed såvel som mod uautoriseret adgang, ændring og spredning.

Artikel 8

Yderligere beskyttelse af den registrerede

Enhver skal have mulighed for:

a. at få kendskab til tilstedeværelsen af et elektronisk register med personoplysninger og dets hovedformål, samt hvem den registeransvarlige er, dennes faste bopæl eller hovedforretningssted;

b. med passende mellemrum og uden unødig forsinkelse eller omkostning at få bekræftet, om der i det elektroniske register er lagret personoplysninger vedrørende den pågældende selv, samt til at blive underrettet om disse data i en forståelig form;

c. at få rettet, henholdsvis slettet, disse oplysninger, hvis de er blevet behandlet i strid med de bestemmelser i national lovgivning, der omhandler de i artikel 5 og 6 anførte grundlæggende principper;

d. klageadgang, hvis anmodning om bekræftelse, underretning, rettelse eller sletning, som anført i litra b og c ikke imødekommes.

Artikel 9

> Undtagelser og begrænsninger
>
> **1.** Artikel 5, 6 og 8 må kun fraviges inden for de i denne artikel anførte grænser.
>
> **2.** Artikel 5, 6 og 8 kan fraviges, når den kontraherende parts gældende lovgivning hjemler det og undtagelsen er en nødvendig forholdsregel i et demokratisk samfund for at:
>
> a. beskytte statens sikkerhed, offentlighedens sikkerhed, statens økonomiske interesser eller for at bekæmpe strafbare forhold;
>
> b. beskytte den registrerede eller andres frihedsrettigheder og andre rettigheder.
>
> **3.** Udøvelsen af de i artikel 8, b, c og d, fastlagte rettigheder kan ved lov begrænses for elektroniske registre med personoplysninger, der benyttes til statistiske eller forskningsmæssige formål, når der ikke åbenbart er fare for, at de registreredes retsbeskyttelse og ret til privatlivets fred herved krænkes." (Lovbekendtgørelse nr. 59, af 16. maj 1991, art. 5-9).

Artiklerne fastsætter således nærmere krav til personoplysningernes beskaffenhed, herunder indsamling og behandling. Proportionalitetsprincippet kommer til udtryk i art. 5, hvoraf det fremgår, at de omfattede oplysninger skal være relevante og tilstrækkelige og ikke omfatte mere end, hvad der kræves til opfyldelsen af de formål, de er lagret til.

I art. 9, der vedrører undtagelser og begrænsninger til de ovennævnte bestemmelser, er anført, at såfremt det er en: "[...] nødvendig forholdsregel i et demokratisk samfund [...]" (Lovbekendtgørelse nr. 59, af 16. maj 1991, art. 9, stk. 2), må art. 5, 6 og 8 fraviges. Denne fravigelse kan omfatte beskyttelse af statens eller offentlighedens sikkerhed, statens økonomiske interesser eller bekæmpelse af strafbare forhold.

5.1.4. Code of Fair Information Practice og The OECD Privacy Framework

Organisationen for Økonomisk Samarbejde og Udvikling (herefter blot OECD) vedtog i 1980 en række principper for privatlivsbeskyttelse, der blev navngivet Guidelines of Protection of Privacy and Transborder Flows of Personal Data.

Disse principper er inspireret af de såkaldte Code of Fair Information Practice (herefter blot FIP), der blev udformet i 1973 af US Secretary's Advisory Committee on Automated Personal Data Systems, der hører under Department of Health, Education & Welfare. FIP er udformet med afsæt i en liberalistisk tanke om, at individet har ret til at kontrollere information om sig selv. Midlerne til denne kontrol er de enkelte principper, som FIP udgøres af (Regan, 2002, s. 397). FIP består af fem internationalt anerkendte principper og blev udformet, da den daværende lovgivning kun i ringe grad beskyttede den enkeltes privathed. FIP-principperne blev offentliggjort i rapporten "Records, Computers and the Rights of Citizens" (1973) og har følgende ordlyd:

> "There must be no personal data record-keeping systems whose very existence is secret.
>
> There must be a way for an individual to find out what information about him is in a record and how it is used.
>
> There must be a way for an individual to prevent information about him that was obtained for one purpose from being used or made available for other purposes without his consent.
>
> There must be a way for an individual to correct or amend a record of identifiable information about him.
>
> Any organization creating, mailitaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuse of the data." (Secretary's Advisory Committee on Automated Personal Data Systems , 1973, s. xx-xxi).

OECD's principper fra 1980 er siden hen blevet revideret, og senest i 2013 udkom en moderniseret udgave heraf i forbindelse med *The OECD Privacy Framework* (OECD, 2013). Ændringer i brugen af personlige data og nye måder at tilgå databeskyttelse har i følge OECD betydet, at denne revision var en nødvendighed (OECD, 2013, s. 19). OECD's Guidelines er som udgangspunkt ikke juridisk bindende, idet der blot er tale om en vejledning. Dog skal det nævnes, at OECD's principper er indeholdt i Europarådets konvention, hvorved en ratificering af konventionen medfører, at OECD's principper bliver bindende og skal følges (Raguse, 2008, s. 12-13).

OECD's guidelines, PART TWO. BASIC PRINCIPLES OF NATIONAL APPLICATION består af nedennævnte otte principper, der er minimumsstandarder, og kan suppleres yderligere (OECD, 2013, s. 14, stk. 6):

> **"Collection Limitation Principle**
>
> 7. There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.
>
> **Data Quality Principle**
>
> 8. Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.
>
> **Purpose Specification Principle**
>
> 9. The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.
>
> **Use Limitation Principle**
>
> 10. Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 9 except:
>
> a) with the consent of the data subject; or
>
> b) by the authority of law.
>
> **Security Safeguards Principle**
>
> 11. Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.
>
> **Openness Principle**
>
> 12. There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

Individual Participation Principle

> 13. Individuals should have the right:
>
> a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to them;
>
> b) to have communicated to them, data relating to them
>
> i. within a reasonable time;
>
> ii. at a charge, if any, that is not excessive;
>
> iii. in a reasonable manner; and
>
> iv. in a form that is readily intelligible to them;
>
> c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and
>
> d) to challenge data relating to them and, if the challenge is successful to have the data erased, rectified, completed or amended.

Accountability Principle

> 14. A data controller should be accountable for complying with measures which give effect to the principles stated" (OECD, 2013, s. 14-15).

Der lægges i principperne vægt på individets ret til at bestemme over egne data, hvilket kommer til udtryk blandt andet i form af samtykke (se princip nummer 7 og princip nummer 10). Samtykke var også nævnt i OECD's principper allerede i forbindelse med 1980-versionen, hvormed et konkret resultat heraf blandt andet blev, at man nu skulle samtykke online til ofte omfattende skriftlige notifikationer.

Sådanne omfattende notifikationer efterfulgt af en forespørgsel om, hvorvidt man vil samtykke hertil, møder man også i dag i sin færden på online. I praksis har de fleste vel svaret ja til, at de har læst og forstået et længere regelsæt i forbindelse med anvendelse af et program, en service eller en webside. Man har da afgivet hvad, der umiddelbart fremstår som et informeret samtykke. I praksis scroller man dog typisk blot ned til bunden af en sådan notifikation og giver til kende, at man er enig (European Commission, 2014a, s. 81-82).

Et eksempel på anvendelse af informeret samtykke online var cookiebekendtgørelsens[121] ikrafttræden i 2011 i Danmark (Lovbekendtgørelse nr. 1148 af 9. december 2011). Cookiebekendtgørelsen er en implementering af det såkaldte e-databeskyttelsesdirektiv[122] (Europa-parlamentets og rådets direktiv, 2002). I forbindelse med en ændring af e-databeskyttelsesdirektivet [123] (Europa-Parlamentets og rådet, 2009) indførtes kravet om informeret samtykke ved lagring af cookies. Af ændringen til e-databeskyttelsesdirektivet fra 2009, art. 5, stk. 3, fremgår det, at:

> "Medlemsstaterne sikrer, at lagring af oplysninger eller opnåelse af adgang til oplysninger, der allerede er lagret i en abonnents eller brugers terminaludstyr, kun er tilladt på betingelse af, at abonnenten eller brugeren har givet sit samtykke hertil efter i overensstemmelse med direktiv 95/46/EF at have modtaget klare og fyldestgørende oplysninger, bl.a. om formålet med behandlingen [...]" (Europa-Parlamentets og rådet, 2009, artikel 5, stk 3).

Formålet med cookie-bekendtgørelsen er, at man sikrer brugerens ret til privatliv igennem informeret samtykke. Idet man beskytter brugernes terminaludstyr, betyder det også, at man anser dette for en del af brugernes privatsfære (Erhvervsstyrelsen, 2013, s. 9). Med cookiebekendtgørelsen regulerer man midlet til indsamling af data – altså cookies (Erhvervsstyrelsen, 2013, s. 13).

I *The OECD Privacy Framework* nævnes ikke *informeret samtykke* (*informed consent*), men blot samtykke (*consent*) (OECD, 2013, princip 7 og princip 10). Man må dog med rimelighed kunne antage, at det, man ifølge principperne sigter imod, er et informeret samtykke – det har trods alt ringe værdi at opstille et princip, der tilsiger, at man skal samtykke til noget, hvis man ikke er informeret herom.

[121] Bekendtgørelsens fulde navn er "Bekendtgørelse om krav til information og samtykke ved lagring af eller adgang til oplysninger i slutbrugeres terminaludstyr" (Lovbekendtgørelse nr. 1148 af 9. december 2011).

[122] E-databeskyttelsesdirektivets fulde navn på dansk er " Europa-Parlamentets og Rådets direktiv 2002/58/EF om behandling af personoplysninger og beskyttelse af privatlivets fred i den elektroniske kommunikationssektor" (Europa-parlamentets og rådets direktiv, 2002).

[123] Ændring af e-databeskyttelsesdirektivet til Europa-Parlamentets og Rådets direktiv 2009/136/EF.

For at kunne vurdere, hvorvidt der reelt afgives et informeret samtykke, må det fastlægges, hvad der forstås herved. Informeret samtykke betyder grundlæggende, som navnet indikerer, at man som individ giver sig samtykke til et givent forhold på baggrund af information herom. Samtykket skal ikke kun opfattes som en positiv respons, men kan også betyde en *informeret afvisning*[124].

Informeret samtykke er en hjørnesten inden for den medicinske verden i relationen mellem sundhedsprofessionel og patient. Det er derfor relevant at skele til, hvordan man kigger på informeret samtykke i den kontekst. Bioetikerene Beauchamp og Childress (2001) har udarbejdet en model for informeret samtykke bestående af to komponenter, informeret og samtykke.[125] Ifølge modellen dækker informeret over: "[...] disclosure of information and comprehension of what is disclosed." (Beauchamp & Childress, 2001, s. 79). Samtykke implicerer: "[...] a voluntary desicion and autorization to proceed." (Beauchamp & Childress, 2001, s. 79).

Informeret samtykke har også været behandlet i forhold til informationssystemer (Friedman, Lin, & Miller, 2005). Der kan i denne kontekst opstilles en model bestående af seks komponenter. De første to trin (*disclosure* og *comprehension*) består i det at blive informeret. De efterfølgende tre trin (*voluntariness*, *competence* og *agreement*) udgør samtykket. Det sidste punkt (*minimal distraction*) implicerer, at brugeren ikke skal distraheres for meget fra brugerens primære opgave (Friedman, Lin, & Miller, 2005, s. 507).

Som nævnt gav OECD's principper anledning til en praksisændring, hvorefter man skulle samtykke online. Selve den tekst, man skal samtykke til, er ofte bevidst besværliggjort ved udelukkende at bestå af versaler og særlig juridisk terminologi (European Commission, 2014a, s. 82, fodnote 294). Det må nødvendigvis være i modstrid med "informeret" ifølge Beauchamps og Childress'

[124] Egen oversættelse af *informed refusal* (Beauchamp & Childress, 2001, s. 80).

[125] Beauchamp og Childress har også udformet en mere omfattende og detaljeret model bestående af syv komponenter (Beauchamp & Childress, 2001, s. 80). Den mere simple model bestående af kun to komponenter synes dog tilstrækkelig som diskussionensgrundlag i ovenstående.

definition, hvis der sker en bevidst besværliggørelse af læsningen af et tekststykke. Godt nok gøres informationen tilgængelig, men det kan aldrig være rimeligt, at den tekst, der skal danne grundlag for et samtykke, bevidst gøres sværere at læse og forstå. Friedman har også i forbindelse med komponenten *comprehension* påpeget det problematiske i at skulle sikre sig, at en person rent faktisk har forstået en information i en teknologisk medieret kommunikation (Friedman, Lin, & Miller, 2005, s. 507-508).

Ifølge Beauchamps og Childress' model implicerer selve samtykket, at en frivillig beslutning om og autorisation til at forsætte en given handling finder sted. Beslutningen er frivillig i den forstand, at individet næppe kan siges at være direkte tvunget til at tage beslutningen. Omvendt kan man overveje, om man står i en reel valgsituation, hvis man kun får adgang til en given service eller webside, hvis man samtykker til en information. Det er muligt at afvise cookies, der er underlagt cookie-bekendtgørelsen. Samtidig er det dog ikke et krav, at en hjemmeside skal kunne eller ville tilbyde sine services uden cookies. Derfor kan en afvisning af cookies betyde, at man som bruger skal forlade en hjemmeside.

At personer skal samtykke online, kan problematiseres mere generelt, idet man kan stille spørgsmålstegn ved, om samtykkekravet anvendes så hyppigt, at det mister sin værdi, idet der sker en "rutinisering". Schermer et al har eksempelvis bemærket, at datasubjekter blot samtykker online, hver gang muligheden foreligger (Schremer, Custers, & van der Hof, 2014, s. 171). Det giver anledning til skepsis om, hvorvidt informeret samtykke reelt virker efter hensigten, og det kan hævdes, at der er mangler sammenhæng mellem den juridiske teori og den praksis, der optræder hos brugerne (Schremer, Custers, & van der Hof, 2014, s. 172).

Man kan i forbindelse hermed overveje, om løsningen er mindre brug af informeret samtykke. Fjernelse af samtykkekravet/-adgangen eller kun sjælden brug heraf betyder, at man fratager borgerne en grad af autonomi. Derved problematiseres i høj grad privathed forstået som retten til selv at bestemme over egne informationer. Begge løsningsmodeller (ofte brug af samtykke og

sjælden brug af samtykke) synes således at implicere en række problemstillinger.

I forlængelse heraf skal det bemærkes, at FN i resolutionen The Right to Privacy in a Digital Age har påpeget, at det har været foreslået, at:

> "[...] the conveyance and exchange of personal information via electronic means is part of a conscious compromise through which individuals voluntarily surrender information about themselves and their relationships in return for digital access to goods, services and information." (Human Rights Council, United Nations, 2014, s. 6, § 18).

I relation til informeret samtykke ville en implementering af en praksis som den, der beskrives i citatet, betyde, at blot idet man anvender en tjeneste, giver man dermed også samtykke til, at der sker en udveksling af data – et tavst samtykke. Antagelsen i argumentet er, at det enkelte individ er bevidst om, at der er tale om et "noget for noget"-kompromis, hvis man som individ får adgang til en given service. Implikationen af en sådan praksis er, at et individ fratages muligheden for at være autonom, såfremt man gør brug af en service.

5.1.5. DIREKTIV 95/46/EF OG 2002/58/EF

Databeskyttelsesdirektivet, Direktiv 95/46/EF[126], blev i 1995 vedtaget i EU og er baseret på OECD's principper fra 1980 – altså på FIP. Helt overordnet er formålet med Databeskyttelsesdirektivet at harmonisere lovgivningen vedrørende beskyttelse af data og at give substans til bestemmelserne om retten til privathed i Konvention 108.

Da Databeskyttelsesdirektivet blev vedtaget, havde flere medlemsstater allerede egne selvstændige databeskyttelseslove. Såfremt en nation allerede havde mere vidtrækkende lovgivning på et specifikt område end foreskrevet ved Databeskyttelsesdirektivet, kunne denne mere vidtrækkende lovgivning bibeholdes. Afgørende er, at alle medlemslande i det Økonomiske Europæiske Sa-

[126] Direktivets fulde navn på dansk er Europa-Parlamentets og Rådets direktiv 95/46/EF af 24. oktober 1995 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (EU). Dette direktiv udgør grundlaget for den danske persondatalov.

marbejdsområde (EØS) som minimum skal følge Direktiv 95/46/EF (Europa-parlamentet og rådets direktiv, 1995; Raguse, 2008, s. 14). Indenfor EU gælder databeskyttelsesdirektivet selvsagt fuldt ud, og det er op til EU-domstolen at bestemme, hvorvidt et land har opfyldt dets forpligtelser i forhold til direktivets bestemmelser. I forholdet mellem EU-lande og øvrige lande finder direktivet ikke anvendelse. Med henblik på at sikre at de principper, som direktivet er funderet på, reflekteres i forholdet med sådanne øvrige lande, er der indgået konkrete aftaler herom, heriblandt den såkaldte Safe Harbor-aftale, der er indgået mellem EU og USA. Denne omtales i afsnit 5.1.7., *EU og USA: Sammenligning af retskilder.*

Databeskyttelsesdirektivet sigter konkret mod at beskytte retten til privatliv for levende personer (Raguse, 2008, s. 14). De oplysninger, som direktivet beskytter, er såkaldte "personoplysninger", der gør en registreret person identificerbar, hvilket er defineret som:

> "[...] enhver form for information om en identificeret eller identificerbar fysisk person (»den registrerede«); ved identificerbar person forstås en person, der direkte eller indirekte kan identificeres, bl.a. ved et identifikationsnummer eller et eller flere elementer, der er særlige for denne persons fysiske, fysiologiske, psykiske, økonomiske, kulturelle eller sociale identitet" (Europa-parlamentet og rådets direktiv, 1995, art. 2, litra a).

Der er ikke kun tale om elektronisk behandling af data, men om behandling af data generelt (Europa-parlamentet og rådets direktiv, 1995, art. 2, litra b).

I Databeskyttelsesdirektivets art. 6, stk. 1, findes en række generelle og grundlæggende principper for databeskyttelse, som er særligt centrale. Art. 6, stk. 1, minder i høj grad om art. 5 i Konvention 108. Art. 6, stk. 1, har følgende ordlyd:

> "1. Medlemsstaterne fastsætter bestemmelser om, at personoplysninger
>
> a) skal behandles rimeligt og lovligt
>
> b) skal indsamles til udtrykkeligt angivne og legitime formål, samt at senere behandling heraf ikke må være uforenelig med disse formål; senere behandling af oplysninger i historisk, statistisk el-

> ler videnskabeligt øjemed anses ikke for at være uforenelig med disse formål, såfremt medlemsstaterne giver de fornødne garantier
>
> c) skal være relevante og tilstrækkelige og ikke omfatte mere end, hvad der kræves til opfyldelse af de formål, hvortil de indsamles, og til de formål, hvortil de senere behandles
>
> d) skal være korrekte og om nødvendigt ajourførte; der skal tages ethvert rimeligt skridt til at slette eller berigtige oplysninger, der er urigtige eller ufuldstændige i forhold til det formål, hvortil de indsamles, eller i forbindelse med hvilke de behandles på et senere tidspunkt
>
> e) ikke må opbevares på en måde, der giver mulighed for at identificere de registrerede i et længere tidsrum end det, der er nødvendigt af hensyn til de formål, hvortil de indsamles, eller i forbindelse med hvilke de behandles på et senere tidspunkt. Medlemsstaterne fastsætter de fornødne garantier for personoplysninger, der i historisk, statistisk eller videnskabeligt øjemed opbevares længere end i ovennævnte periode." (Europa-parlamentet og rådets direktiv, 1995, art. 6, stk 1).

Som udgangspunkt skal al anden databeskyttelseslovgivning i EU være i overensstemmelse med ovenstående. I henhold til art. 13, der vedrører Undtagelser og begrænsninger, kan art. 6, stk. 1, dog begrænses i visse tilfælde:

> "Artikel 13
>
> Undtagelser og begrænsninger
>
> 1. Medlemsstaterne kan træffe lovmæssige foranstaltninger med henblik på at begrænse rækkevidden af de forpligtelser og rettigheder, der er omhandlet i artikel 6, stk. 1, artikel 10, artikel 11, stk. 1, samt artikel 12 og 21, hvis en sådan begrænsning er en nødvendig foranstaltning af hensyn til:
>
> a) statens sikkerhed
>
> b) forsvaret
>
> c) den offentlige sikkerhed
>
> d) forebyggelse, efterforskning, afsløring og retsforfølgning i straffesager eller i forbindelse med brud på etiske regler for lovregulerede erhverv

> e) væsentlige økonomiske eller finansielle interesser hos en medlemsstat eller Den Europæiske Union, herunder valuta-, budget- og skatteanliggender
>
> f) en kontrol-, tilsyns- eller reguleringsopgave, selv af midlertidig karakter, der er et led i den offentlige myndighedsudøvelse på de i litra c), d) og e) nævnte områder
>
> g) beskyttelsen af den registreredes interesser eller andres rettigheder og frihedsrettigheder." (Europa-parlamentet og rådets direktiv, 1995, art. 13, stk 1).

Af art. 17, der vedrører behandlingssikkerhed, fremgår det endvidere, at den registeransvarlige[127] skal fastsætte fornødne tekniske og organisatoriske foranstaltninger til at beskytte personoplysninger mod: "[...] hændelig eller ulovlig tilintetgørelse, mod hændeligt tab, mod forringelse, ubeføjet udbredelse eller ikke-autoriseret adgang [...]" (Europa-parlamentet og rådets direktiv, 1995, art. 17, stk 1). Desuden giver Databeskyttelsesdirektivet mulighed for, at en registreret person har retten til at få indsigt i personoplysninger:

> "Artikel 12
>
> Ret til indsigt
>
> Medlemsstaterne sikrer enhver registreret ret til hos den registeransvarlige
>
> a) frit og uhindret, med rimelige mellemrum og uden større ventetid eller større udgifter
>
> - at få oplyst, om der behandles personoplysninger om den pågældende selv, samt mindst formålene med behandlingen, hvilken type oplysninger det drejer sig om, og modtagerne eller kategorierne af modtagere af oplysningerne

[127] Ifølge databeskyttelsesdirektivets art. 2, litra d, er den registeransvarlige den "[...] fysiske eller juridiske person, offentlige myndighed, institution eller ethvert andet organ, der alene eller sammen med andre afgør, til hvilket formål og med hvilke hjælpemidler der må foretages behandling af personoplysninger; [...]" (Europa-parlamentet og rådets direktiv, 1995, art. 2, litra d). En såkaldt registerfører er i følge art. 2, litra e, den "[...] fysiske eller juridiske person, offentlige myndighed, institution eller ethvert andet organ, der behandler personoplysninger på den registeransvarliges vegne [...]" (Europa-parlamentet og rådets direktiv, 1995, art. 2, litra e).

> - at få meddelt letforståelig information om, hvilke oplysninger der er omfattet af behandlingerne, samt enhver tilgængelig information om, hvorfra disse oplysninger stammer
>
> - at få at vide, hvilken logik der ligger bag edb-behandlingen af oplysningerne om den pågældende, i det mindste i forbindelse med edb-baserede afgørelser som omhandlet i artikel 15, stk. 1
>
> b) efter omstændighederne at få oplysninger, som ikke er blevet behandlet i overensstemmelse med dette direktiv, berigtiget, slettet eller blokeret, navnlig hvis de er ufuldstændige eller urigtige
>
> c) at få udvirket, at tredjemand, til hvem sådanne oplysninger er blevet videregivet, underrettes om enhver berigtigelse, sletning eller blokering, der er foretaget i overensstemmelse med litra b), medmindre underretning viser sig umulig eller er uforholdsmæssig vanskelig." (Europa-parlamentet og rådets direktiv, 1995, art. 12).

Generelle betingelser i Databeskyttelsesdirektivet finder også anvendelse i forhold til sikkerhedsteknologier (Raguse, 2008, s. 20).

Udover Direktiv 95/46/EF er også et andet EU-direktiv relevant for afhandlingens emne. Der er tale om Direktiv 2002/58/EF, Direktiv om databeskyttelse inden for elektronisk kommunikation[128] (Europa-parlamentets og rådets direktiv, 2002). Direktivet omhandler specifikt databeskyttelse i forhold til elektronisk kommunikation. Dette direktiv sigter overordnet mod at sikre rettighederne omfattet af art. 7 og 8 i Den Europæiske Unions Charter om Grundlæggende Rettigheder (Europa-parlamentets og rådets direktiv, 2002).

Direktivet har som formål at sikre borgernes tillid til de services og teknologier, der anvendes i forbindelse med elektronisk kommunikation. Direktivet indførtes som en reaktion på, at nye avancerede teknologier blev taget i brug i det offentlige, hvorved der opstod et særligt behov for beskyttelse af brugernes personoplysninger (Europa-parlamentets og rådets direktiv, 2002). Direktivets bestemmelser omhandler primært såkaldte trafikdata, der defineres som: "[...] data, som behandles med henblik på overføring af kommunikation i

[128] Dele af bestemmelserne i dette direktiv er flyttet til den såkaldte ændringsakt, Direktiv 2006/24/EF, bedre kendt som Logningsdirektivet. Dette direktiv er omtalt tidligere i afhandlingen.

et elektronisk kommunikationsnet eller debitering heraf." (Europa-parlamentets og rådets direktiv, 2002, art. 2, b), og lokaliseringsdata, der defineres som: "[...] data, som behandles i et elektronisk kommunikationsnet og angiver den geografiske placering af det terminaludstyr, som brugeren af en offentligt tilgængelig elektronisk kommunikationstjeneste anvender" (Europa-parlamentets og rådets direktiv, 2002, art. 2, litra c). Ydermere beskyttes også telefonopkald og elektronisk post. Som for Direktiv 95/46/EF gælder det også for 2002/58/EF, at såfremt det er nødvendigt eksempelvis for at opretholde statens sikkerhed, kan beskyttelsen begrænses (Europa-parlamentets og rådets direktiv, 2002, s. 38).

5.1.5.1. DATABESKYTTELSE: INDIREKTE IDENTIFIKATION OG ANONYMISERING

Et problem i dag i forhold til databeskyttelse er blandt andet indirekte identifikation af personer. EU's databeskyttelsesdirektiv beskytter levende personer og:

> "[...] enhver form for information om en identificeret eller identificerbar fysisk person (»den registrerede«); **ved identificerbar person forstås en person, der direkte eller indirekte kan identificeres** [...]"(min fremhævelse) (Europa-parlamentet og rådets direktiv, 1995, art. 2, litra a).

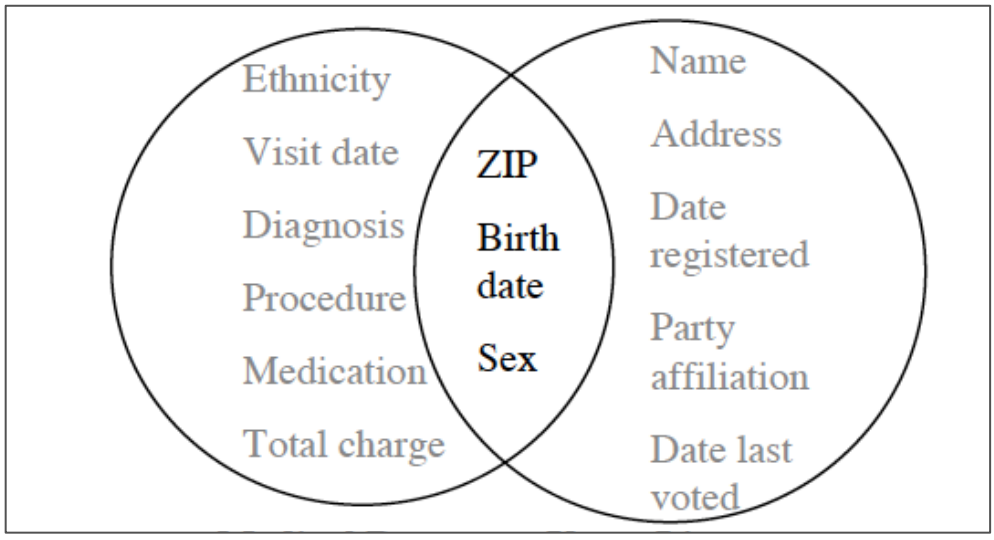
Dette betyder, at såfremt en person kan identificeres indirekte, er denne omfattet af databeskyttelsesdirektivet og er at betragte som et datasubjekt. På baggrund af data, der ikke indeholder direkte personlige data, kan man ved anvendelse databehandling og sammenkørsel af data, finde frem til personlige informationer om en specifik person (Mayer-Schönberger & Cukier, 2013, s. 152).

Der findes tekniske løsninger, hvormed man søger at afhjælpe dette problem. Blandt andet såkaldt *anonymisering.* Grundlæggende er ideen med anonymisering, at man fjerner alle de data, der kan identificere en unik person: Kreditkort-informationer, cpr-nummer, navn, adresse, telefonnummer og så videre. Derudover skal anonymisering også sikre, at man ikke *utilsigtet* og/eller *indirekte* kan identificere en person. Det er her den reelle udfordring opstår. Data, der ikke umiddelbart har karakter af, at man på baggrund af disse kan identi-

ficere personer, tillader i mange tilfælde alligevel en re-identificering af personer, hvis man matcher data med anden data (Sweeney, 2002, s. 557-558). Eksempelvis er det bevist, at 87 procent af den amerikanske befolkning på 246 millioner i 1990 principielt kunne identificeres unikt blot ved at have information om deres postnummer, køn og fødselsdato (Sweeney, 2002, s. 558).

Et andet eksempel på anonymisering og re-identifikation af data stammer fra USA, hvor Sweeney har demonstreret, hvordan det var muligt at identificere den tidligere guvernør i Massachusetts ved at have to eftersigende anonymiserede datasæt til sin rådighed (Sweeney, 2002, s. 558). I Massachusetts indsamlede forsikringsselskabet Group Insurance Commision data om statsansatte i forbindelse med indkøb af forsikringer til statsansatte. Eksempler på de data, der blev indsamlet, fremgår af den venstre cirkel på billede 6. Idet forsikringsselskabet mente, at dets data om de enkelte statsansatte var anonymiserede, blev kopier givet til blandt andet forskere (Sweeney, 2002, s. 558).

Den højre cirkel på billede 6 illustrerer den information, som et datasæt der kunne købes i Massachusetts omhandlende registrerede vælgere Cambridge, indeholdt (Sweeney, 2002, s. 558).



Billede 6: Eksemplificering af anonymiseringsproblem (Sweeney, 2002, s. 559)

Idet begge datasæt indeholdt information om postnummer, fødselsdato og køn – den fællesmængde, der fremgår på billede 6 – kunne de efterfølgende

forbindes. Sundhedsoplysninger vedrørende den daværende guvernør i Massachusetts var på forsikringsselskabets eftersigende anonymiserede liste. Det viste sig, at der mellem de to lister kun var sammenfald for seks personer for så vidt angik deres fødselsdato, og heraf var der kun tre datasubjekter, der var mænd. Af disse tre mænd var Guvernør Wels den eneste, der var bosiddende i et bestemt postnummer (Sweeney, 2002, s. 559). Således kunne guvernøren identificeres på baggrund af oplysningerne fra de to eftersigende anonymiserede datasæt.

En måde, hvorpå problematikken kunne være undgået, er ved at anvende den konkrete data-anonymiseringsmetode, *k-anonymisering* [129] . Ved k-anonymisering sikres, at et datasubjekt ikke kan differentieres i blandt *k* andre. I ovennævnte tilfælde ville kombinationen af fødselsdato, køn og postnummer derved ikke havde givet sig udslag i én unik, identificerbar person – det ville have givet *k* (Sweeney, 2002). Havde man eksempelvis i det ovennævnte tilfælde anvendt fødselsårstal i stedet for den fulde fødselsdato, havde det ikke været muligt at identificere guvernøren.

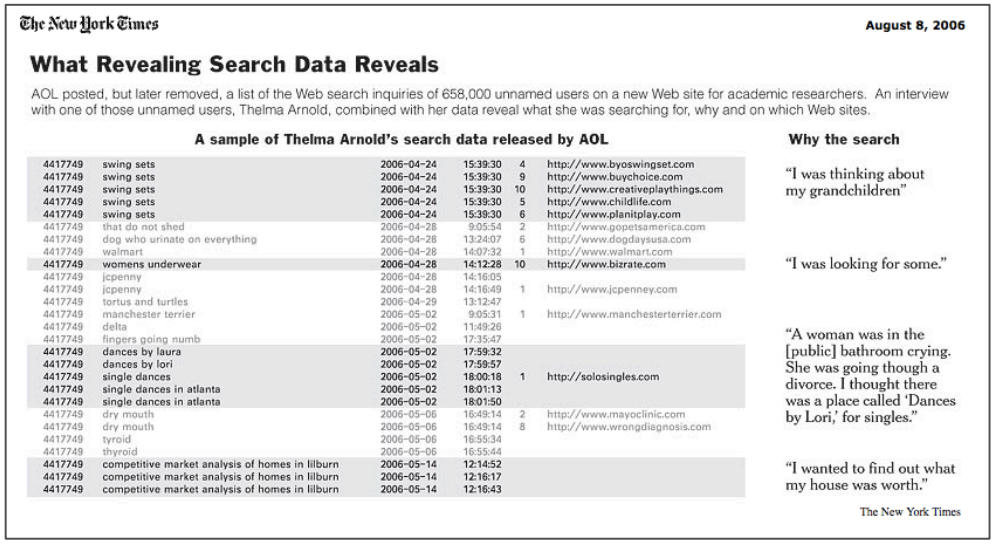
Anvendelse af k-anonymisering sikrer dog ikke *nødvendigvis* altid anonymitet. Man kan forestille sig en situation hvor k = 2, men hvor den sensitive attribut er den samme for to entiteter i en klasse.[130] Det er således svært at sikre sig mod alle scenarier.

Et andet eksempel på utilstrækkelig anonymisering af data er, da søgemaskinen AOL intentionelt frigjorde 20 millioner søgninger, der var foretaget over tre måneder. Formålet var at stille data til rådighed for forskning, hvilket man valgte at gøre ved at offentliggøre disse på internettet. AOL havde tilskrevet brugerne et ID med henblik på at sikre deres anonymitet. Forventningen var, at idet man havde fjernet alle eksplicitte identifikatorer, fremstod disse data som anonyme. Det viste sig hurtigt ikke at være tilstrækkeligt. New York Times fandt frem til en bruger med ID-nummer 4417749 på baggrund af bruge-

[129] Fra det engelske "k-anonymization" (Sweeney).

[130] Der eksisterer metoder, hvormed dette problem kan løses. Det ligger uden for afhandlingen område at diskutere disse metoder i flere detaljer.

rens søgninger. Der var tale om en på det tidspunkt 62-årig kvinde ved navn Thelma Arnold, der var bosiddende i Lilburn, Georgia, USA. Hun havde blandt andet søgt på "Landscapers in Lilburn, Ga,", "homes sold in shadow lake subdivision gwinnett county georgia.", "60 single men" og "the best season to visit Italy" (Barbaro & Zeller, 2006). Billede 7 viser en oversigt over nogle af de søgninger, som Arnold foretog, og som AOL offentliggjorde.



The New York Times — August 8, 2006

What Revealing Search Data Reveals

AOL posted, but later removed, a list of the Web search inquiries of 658,000 unnamed users on a new Web site for academic researchers. An interview with one of those unnamed users, Thelma Arnold, combined with her data reveal what she was searching for, why and on which Web sites.

A sample of Thelma Arnold's search data released by AOL

4417749	swing sets	2006-04-24	15:39:30	4	http://www.byoswingset.com
4417749	swing sets	2006-04-24	15:39:30	9	http://www.buychoice.com
4417749	swing sets	2006-04-24	15:39:30	10	http://www.creativeplaythings.com
4417749	swing sets	2006-04-24	15:39:30	5	http://www.childlife.com
4417749	swing sets	2006-04-24	15:39:30	6	http://www.planitplay.com
4417749	that do not shed	2006-04-28	9:05:54	2	http://www.gopetsamerica.com
4417749	dog who urinate on everything	2006-04-28	13:24:07	6	http://www.dogdaysusa.com
4417749	walmart	2006-04-28	14:07:32	1	http://www.walmart.com
4417749	womens underwear	2006-04-28	14:12:28	10	http://www.bizrate.com
4417749	jcpenny	2006-04-28	14:16:05		
4417749	jcpenny	2006-04-28	14:16:49	1	http://www.jcpenney.com
4417749	tortus and turtles	2006-04-29	13:12:47		
4417749	manchester terrier	2006-05-02	9:05:31	1	http://www.manchesterterrier.com
4417749	delta	2006-05-02	11:49:26		
4417749	fingers going numb	2006-05-02	17:35:47		
4417749	dances by laura	2006-05-02	17:59:32		
4417749	dances by lori	2006-05-02	17:59:57		
4417749	single dances	2006-05-02	18:00:18	1	http://solosingles.com
4417749	single dances in atlanta	2006-05-02	18:01:13		
4417749	single dances in atlanta	2006-05-02	18:01:50		
4417749	dry mouth	2006-05-06	16:49:14	2	http://www.mayoclinic.com
4417749	dry mouth	2006-05-06	16:49:14	8	http://www.wrongdiagnosis.com
4417749	tyroid	2006-05-06	16:55:34		
4417749	thyroid	2006-05-06	16:55:44		
4417749	competitive market analysis of homes in lilburn	2006-05-14	12:14:52		
4417749	competitive market analysis of homes in lilburn	2006-05-14	12:16:17		
4417749	competitive market analysis of homes in lilburn	2006-05-14	12:16:43		

Why the search

"I was thinking about my grandchildren"

"I was looking for some."

"A woman was in the [public] bathroom crying. She was going though a divorce. I thought there was a place called 'Dances by Lori,' for singles."

"I wanted to find out what my house was worth."

The New York Times

Billede 7: Nogle af Arnolds søgninger som AOL offentliggjorde (Link via Barbaro & Zeller, 2006).

Allerede 3 dage efter lækket valgte AOL at fjerne de offentliggjorte data fra nettet igen, da problemerne begyndte at melde sig (Wikipedia, AOL search data leak). Disse data var dog allerede blevet spredt og kopieret og kan derved principielt florere online for altid.

Der findes også andre teknikker til at beskytte data. Eksempelvis *randomisering*[131], hvor man "skjuler" de egentlige data ved at tilføje statistisk støj. Ydermere findes også såkaldte *kryptografiske modeller*[132], hvormed den generelle ide er, at man kun viser resultater af dataanalyse, men aldrig de faktiske data (Giannotti, Monreale, & Pedreschi, 2013, s. 177-178). De ovennævnte eksem-

[131] Egen oversættelse af "randomization" (Giannotti, Monreale, & Pedreschi, 2013, s. 177).

[132] Egen oversættelse af "cryptography-based models" (Giannotti, Monreale, & Pedreschi, 2013, s. 177-178).

pler illustrerer dog, at anonymisering af data grundlæggende kan være problematisk, eftersom dataene kan de-anonymiseres (Klitou, 2014, s. 270).

5.1.6. NY DATABESKYTTELSESFORORDNING I EU

Netop nedenfor vil jeg kort redegøre for et endnu ikke gennemført forslag til en EU-forordning. Forslaget blev fremlagt af Europa-Kommissionen den 25. januar 2012 (European Commission, 2012). Med forslaget har kommissionen forsøgt i højere grad at forene individets privathed og udnyttelse af nye teknologiske muligheder samt at modernisere det nuværende databeskyttelsesdirektiv, Direktiv 95/46/EF (Europa-parlamentet og rådets direktiv, 1995), idet dette anses for at være forældet. Det er ikke så underligt, at en modernisering er på sin plads, når man påtænker teknologiens udvikling i de tyve år, der er gået, siden det gældende direktiv blev implementeret i 1995. Den konstante udvikling af nye informations- og kommunikationsteknologier sætter lovgivningen under pres (ARTICLE 29 Data Protection Working Party, 2009). Ydermere udfordres lovgivningen af ønsket om harmonisering, globalisering og internationalt samarbejde (Lyon, 2007, s. 196; van den Hoven, 2013; van den Hoven, 1999, s. 139).

Formålet med den nye forordning er, at databeskyttelseslovgivningen i højere grad end nu harmoniseres EU-landene imellem, således at der i EU er ét fælles regelsæt vedrørende databeskyttelse (European Commission, 2014b). Det står i modsætning til, at der på nuværende tidspunkt eksisterer 28 forskellige implementeringer af direktiv 95/46/EF. Det forventes på den baggrund, at forslaget vil gøre det nemmere for virksomheder at navigere. Desuden vil virksomheder, der er hjemmehørende uden for EU og som vil drive forretning i EU, i henhold til den nye lovpakke skulle leve op til de samme regler som virksomheder hjemmehørende i EU (European Commission, 2014b). Gør disse virksomheder ikke det, vil overtrædelsen kunne straffes med bøde på op til 5 procent[133] af virksomhedens årlige omsætning. På nuværende tidspunkt bli-

[133] Europa Parlamentet har forslået, at det netop bliver de her omtalte 5 procent af et firmas årlige omsætning, der skal være maksimal størrelse på en bøde. Tidligere har Europa kommissionen foreslået, at det skulle være op til 2 procent af et firmas årlige omsætning.

ver overtrædelser af Databeskyttelsesdirektivet ikke i særlig høj grad sanktioneret (European Commission, 2014b, s. 5; Solove, 2012).

Forslaget indeholder flere væsentlige tiltag. Et af de væsentligste af disse er, at enkelte borgers mulighed for at have kontrol over egne personoplysninger øges. Ideen om at give individet en større grad af kontrol med egne informationer har blandt andet givet sig udslag i den meget omdiskuterede ret til at blive glemt online, måske bedre kendt under det fængende engelske navn: *The right to be forgotten*. Denne ikke absolutte ret til at blive glemt betyder, at:

> "When you no longer want your data to be processed and there are no legitimate grounds for retaining it, the data will be deleted. This is about empowering individuals, not about erasing past events or restricting freedom of the press." (European Commission, 2014b, s. 3).

Retten til at blive glemt online har blandt andet til formål at selvstændiggøre borgeren (European Commission, 2014b, s. 3). Baggrunden er, at det ikke er nemt at slippe fri af sin fortid på internettet, eftersom internettet "husker", hvad der er sket for længe siden. Der er således tale om en anerkendelse af, at alle ændrer sig over tid, og at det kan være ubehageligt at være låst til en person, som man ikke længere kan identificere sig med (Rosen, 2012, s. 88). Man kan f.eks. forestille sig en teenager, der lægger billeder på nettet, som teenageren senere i livet fortryder. Muligheden for at få fjernet indhold på internettet, som man selv har lagt ud, virker i sådan en sammenhæng meget tiltalende for den enkelte.

Retten til at blive glemt online giver anledning til overvejelse om, hvorvidt man har en ret til at få fjernet indhold online, som en anden person har lagt på nettet omhandlende en selv. I USA er svaret på nuværende tidspunkt nej – her kan man ikke forbyde nogen at lægge information på nettet om en, selvom informationen måske er krænkende for en, så længe denne information er opnået på lovlig vis (Rosen, 2012, s. 91). Ej heller kan man kræve sådant offentliggjort materiale fjernet. I forslaget til den nye regulering af data er derimod anført, at: "'personal data' means any information relating to a data subject"; (European Commission, 2012, art. 4, stk. 2). Det forekommer oplagt

at forstå dette som omfattende oplysninger om den enkelte, som andre har lagt på nettet, således at sådanne oplysninger vil kunne kræves fjernet.

Retten til at blive glemt rejser dog et betydeligt problem. Der er i yderste konsekvens tale om en ret til at foretage censur af information. En anerkendelse af eksempelvis retten til at fjerne et billede på et socialt medie kan lede til, at der også gives adgang til at fjerne indhold på en side som Wikipedia. Det betyder, at retten til at blive glemt måske ligefrem kan anvendes til at omskrive historien (Warnier, Dechesne, & Brazier, 2015, s. 436). Dermed rejser retten til at blive glemt en problemstilling, der omhandler både censur og ytringsfrihed.

Yderligere et væsentligt tiltag er, at den nye lovpakke lægger op til, at teknologier, der kan beskytte privatlivets fred, skal tilskyndes. Sådanne teknologier kan være standardindstillinger på websites, der favoriserer privatheden for individet, hvilket er kendt under navnet *Privacy by Default* (European Commission, 2012). Der kan også være tale om ordninger, hvorved det bliver muligt for virksomheder at blive certificeret i forhold til deres privathedsfremmende foranstaltninger (European Commission, 2012, art. 39).

5.1.7. EU OG USA: SAMMENLIGNING AF RETSKILDER

Der er særdeles divergerende måder at tilgå databeskyttelse på globalt. Dette bliver eksplicit, hvis man sammenligner de europæiske og amerikanske retskilder på området. Til trods for at reguleringen i både EU og USA tager afsæt i FIP, er implementeringerne heraf yderst forskellige. I modsætning til i EU har man i USA ikke en overordnet lovgivning vedrørende databeskyttelse.

I EU har man en deontologisk funderet ret til beskyttelse af privathed. Deri ligger, at man beskytter privathed, til trods for at det kan have betydelige økonomiske omkostninger. I USA har man derimod en mere utilitaristisk inspireret virksomhedsvenlig model, hvor man håber, at en mindre restriktiv tilgang kan øge nytten for flest mulige (Ess, 2009, s. 55-56).[134]

[134] Et perspektiv som det amerikanske kan også findes i Richard Posner , der argumenterer for en økonomisk inspireret virksomhedsvenlig privathedsmodel (Posner, 1984). Posner mener, at organisationers privathed er vigtigere end individers privathed. Individer, der får en ret til privathed, kan anvende denne med henblik på at vildlede andre om deres

En helt grundlæggende forskel består i, at man i EU beskytter data. Såfremt det enkelte individ ikke er interesseret i databeskyttelse, skal EU-reguleringen stadig opretholdes og overholdes. Man beskytter således individet i kraft af beskyttelse af data. Derimod findes der i USA blot en række føderale love, der sigter mod beskyttelse af privathed indenfor forskellige sektorer. Eksempelvis reguleres sundhedsrelaterede data med "The Health Insurance Portability and Accountability Act of 1996" (også kendt som HIPAA), og børns (under 13 år) privathed online reguleres med "Childrens Online Privacy Protection Act" (også kendt som COPPA).

Der er dog også sektorer, hvor der ingen føderale databeskyttelseslove er, og hvor det udelukkende er op til den enkelte stat at lovgive. Der er således tale om en langt mere selvregulerende juridisk model, hvor de enkelte virksomheder også selv kan erklære deres egne privathedsløfter, hvis de ønsker det. Såfremt de enkelte virksomheder ikke overholder deres selverklærede privathedsløfter, kan disse virksomheder blive straffet af *Federal Trade Commision* (FTC). Mange virksomheder er derfor påpasselige med at give sådanne løfter (Solove, 2012).

Den europæiske databeskyttelsesmodel er anset for at udgøre en stærkere beskyttelse af data end den amerikanske. Nissenbaum påpeger dog, at hun foretrækker den amerikanske sektorale tilgang (Nissenbaum, 2010, s. 237-238). Det er for så vidt ikke overraskende, at Nissenbaum er tilhænger af en sektoral tilgang til privathed, da det korresponderer med hendes ide om privathed som noget, der er relativt til kontekster. Nissenbaums krav, for at denne tilgang vil fungere, er, at kontektuel integritet anvendes som et generelt princip, nemlig retten til kontektuel integritet (Nissenbaum, 2010, s. 237-238).

Efter terrorangrebet på Manhattan den 11. september 2001 sænkede man i USA kravene til retshåndhævende myndigheders indsamling af personlige

---

egen karakter. Posner mener, at personer ønsker at manipulere den omkringliggende verden ved kun at fortælle udvalgte informationer om dem selv (Posner, 1984, s. 334-335). (Originalkilden blev publiceret første gang i 1978.).

data ved indførelsen af "USA Patriot Act"[135], der blev underskrevet af præsident George W. Bush den 26. oktober 2001.[136] USA Patriot Act betød i praksis, at man kan tilbageholde personer uden sigtelse og overvåge telefoner og internet uden en dommerkendelse.

Som en konsekvens af de særdeles divergerende databeskyttelsesniveauer i henholdsvis USA og EU har man valgt at udforme såkaldte "Safe Harbor Privacy Principles", hvormed man sikrer, at amerikanske virksomheder lever op til Direktiv 95/46/EF, når data flyttes mellem EU og USA. Principperne er dog kun gældende for virksomheder, der også er underlagt US Federal Trade Commission. Af sektion 5, Exceptions i FTC Act fremgår det, at hvilke typer af virksomheder *ikke* er underlagt FTC:

> "[...] financial institutions, including banks, savings and loans, and credit unions;
>
> telecommunications and interstate transportation common carriers;
>
> air carriers; and
>
> packers and stockyard operators." (Export.gov, 2009).

Et ikke ubetydeligt antal af virksomhedssektorer falder således uden for FTC og er dermed heller ikke underlagt Safe Harbor-aftalen. Det er værd at bemærke, at blandt disse ikke-omfattede sektorer er banker og teleselskaber – sektorer, hvor der i stort omfang produceres data, der må formodes at være interessante ud fra et overvågningsperspektiv.

De syv principper indeholdt i Safe Harbor Privacy Principles er ikke juridisk bindende og er i øvrigt implementeret som en selv-certificerende model, som det er frivilligt for amerikanske organisationer, om de ønsker at tage del i. Såfremt de ønsker dette, skal de følge de syv "Safe Harbor Privacy Principles", der har følgende ordlyd:

---

[135] Forkortelse af "**U**niting and **S**trengthening **A**merica by **P**roviding **A**ppropriate **T**ools **R**equired to **I**ntercept and **O**bstruct **T**errorism **A**ct of 2001".

[136] "USA Patriot Act" var udformet før 9/11, men efter terrorangrebet blev denne lov hastet igennem det amerikanske retssystem.

" **1. Notice**

Organizations must notify individuals about the purposes for which they collect and use information about them. They must provide information about how individuals can contact the organization with any inquiries or complaints, the types of third parties to which they disclose the information and the choices and means the organization offers for limiting its use and disclosure.

2. Choice

Organizations must give individuals the opportunity to choose (opt out) whether their personal information will be disclosed to a third party or used for a purpose incompatible with the purpose for which it was originally collected or subsequently authorized by the individual. For sensitive information, affirmative or explicit (opt in) choice must be given if the information is to be disclosed to a third party or used for a purpose other than its original purpose or the purpose authorized subsequently by the individual.

3. Onward Transfer (Transfers to Third Parties)

To disclose information to a third party, organizations must apply the notice and choice principles. Where an organization wishes to transfer information to a third party that is acting as an agent, it may do so if it makes sure that the third party subscribes to the Safe Harbor Privacy Principles or is subject to the Directive or another adequacy finding. As an alternative, the organization can enter into a written agreement with such third party requiring that the third party provide at least the same level of privacy protection as is required by the relevant principles.

4. Access

Individuals must have access to personal information about themselves that an organization holds and be able to correct, amend, or delete that information where it is inaccurate, except where the burden or expense of providing access would be disproportionate to the risks to the individual's privacy in the case in question, or where the rights of persons other than the individual would be violated.

5. Security

Organizations must take reasonable precautions to protect personal information from loss, misuse and unauthorized access, disclosure, alteration and destruction.

6. Data integrity

> Personal information must be relevant for the purposes for which it is to be used. An organization should take reasonable steps to ensure that data is reliable for its intended use, accurate, complete, and current.
>
> **7. Enforcement**
>
> In order to ensure compliance with the Safe Harbor Privacy Principles, there must be (a) readily available and affordable independent recourse mechanisms so that each individual's complaints and disputes can be investigated and resolved and damages awarded where the applicable law or private sector initiatives so provide; (b) procedures for verifying that the commitments companies make to adhere to the Safe Harbor Privacy Principles have been implemented; and (c) obligations to remedy problems arising out of a failure to comply with the Safe Harbor Privacy Principles. Sanctions must be sufficiently rigorous to ensure compliance by the organization. Organizations that fail to provide annual self-certification letters reaffirming their commitment to the U.S.-EU Safe Harbor Framework and/or the U.S.-Swiss Safe Harbor Framework will no longer be assured of the relevant Safe Harbor benefits and may ultimately be removed from the list of participants maintained on the Safe Harbor website." (U.S. Department of Commerce).

Safe Harbor-aftalen er dog kommet under pres i forbindelse med afsløringerne af USA's masseovervågning, der også involverer overvågning af EU-borgere. ARTICLE 29 Data Protection Working Party gør det klart, at masseovervågning ikke er kompatibelt med fundamental databeskyttelseslovgivning. Desuden er opfattelsen, at hverken national sikkerhed eller terrorisme kan retfærdiggøre sådan overvågning. Begrænsninger i forhold til borgeres rettigheder kan kun forsvares, hvis de er proportionale og strengt nødvendige (ARTICLE 29 Data Protection Working Party, 2014, s. 2). Safe Harbor-aftalen sigter mod kommerciel behandling af data, og dette juridiske instrument var ikke designet til at beskytte efterretningstjenesters brug af kommercielle, amerikanske virksomheders data. Article 29 Data Protection Working Party gør det klart, at:

> "Neither Safe Harbor, nor Standard Contractual Clauses, nor BCRs could serve as a legal basis to justify the transfer of personal data to a third country authority for the purpose of massive and indiscriminate surveillance." (ARTICLE 29 Data Protection Working Party, 2014, s. 3).

I USA er statslige organisationers indsamling og anvendelse af data reguleret af den såkaldte Privacy Act of 1974, der trådte i kraft september 1975. Formålet med Privacy Act of 1974 er at begrænse adgangen til information for *federel agencies*, og regelsættet finder anvendelse på amerikanske statsborgere og personer med permanent ophold i USA. En række undtagelser knytter sig dog til Privacy Act of 1974, heriblandt en undtagelse vedrørende såkaldte retshåndhævende formål. Blandt andet betyder det, at en potentielt kriminel person, der er under overvågning, ikke kan få indsigt i filer, der har forbindelse med undersøgelsen af denne person (Electronic Privacy Information Center, 2015).

I modsætning til en informationel forståelse af privathed har man tidligere i amerikansk regulering på området i højere grad set på privathed som et spørgsmål om "ikke-indtrængen"[137] i en mere fysisk forstand. Dette tilsvarer den måde, hvorpå privathed er beskyttet i The Fourth Amendment to The U.S. Constitution. Denne amendment beskytter:

> "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." (United States Courts).

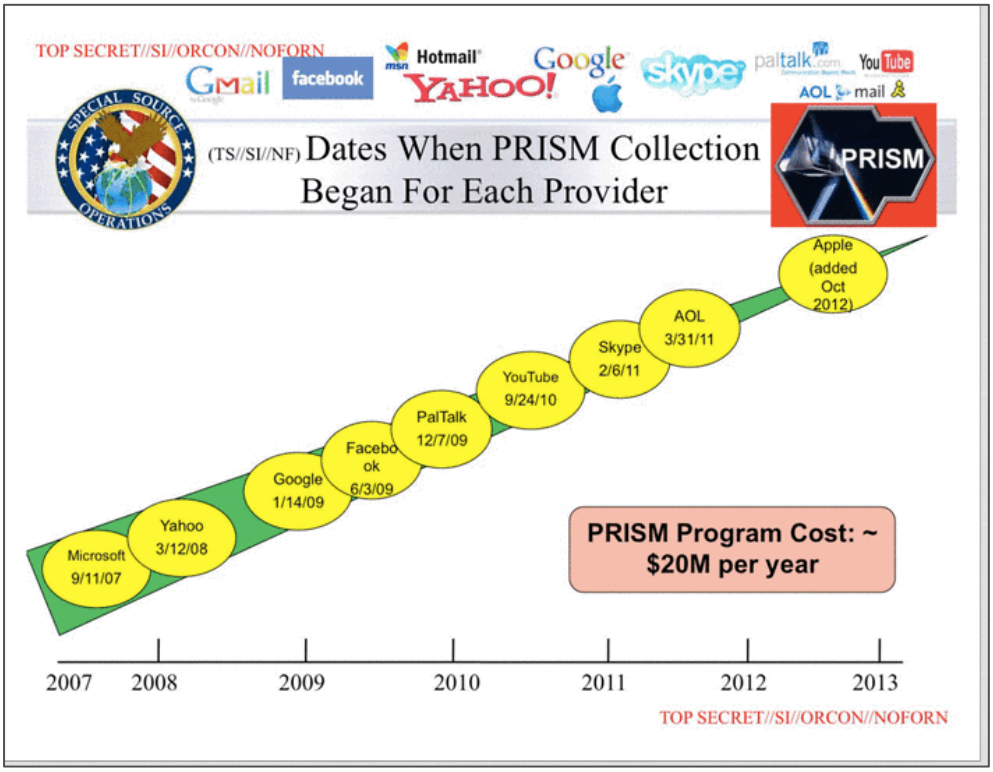
Senere er privathedslovgivningen i USA i højere grad blevet fokuseret på privathed som et spørgsmål om autonomi, eller det som Moor benævner ikke-indblanding[138], hvilket kan eksemplificeres med kvinders ret til at vælge en abort (Moor J. H., 1997, s. 30).

Endvidere har EU-lande og USA forskellige forudsætninger for at overvåge data. En række store virksomheder, der tilbyder forskellige services, er nemlig amerikanske, hvilket betyder, at en meget stor mængde data gemmes på servere i USA. Derved har USA en helt særlig og central position i forhold til databeskyttelse. Som antydet ovenfor giver den amerikanske lovgivning myndig-

[137] Egen oversættelse af "non-intrusion" (Moor J. H., 1997, s. 30).

[138] Egen oversættelse af "non-interference" (Moor J. H., 1997, s. 30).

hederne en relativt vid adgang til dataovervågning. Eksempelvis har det amerikanske NSA teknologien PRISM til deres rådighed. PRISM kan bruges til at indsamle data om specifikke personer igennem specifikke virksomheder. Ifølge slides som Edward Snowden har gjort tilgængelige, er det muligt for NSA at indsamle data fra virksomheder såsom Microsoft, Facebook, Google, Youtube og Apple. Alle virksomheder fremgår af nedestående billede 8



Billede 8: PRISM Slide fra The guardian:
http://www.theguardian.com/world/interactive/2013/nov/01/prism-slides-nsa-document

Til sammenligning har man i eksempelvis Sverige også ret til at indsamle data, når data passerer igennem Sverige (Hypponen, 2013).[139] I tilfælde, hvor USA kritiseres for sin liberale databeskyttelsesregulering (eller fuldstændige mangel på databeskyttelseslovgivning), kan amerikanerne bringe et argument i spil, der siger, at USA ikke er det eneste land, der har adgang til at indsamle data, når data passerer igennem landet – og det har man i USA ret i. Det ændrer dog ikke ved, at der er tale om en ubalance (Hypponen, 2013). Hypponen

[139] Denne lov benævnes i daglig tale FRA-loven (Prop. 2006/07:63) efter navnet på den svenske myndighed, der indssamler data – Försvarets radioanstalt.

eksemplificerer dette med en svensk politiker eller forretningsmand. Det må antages at være overvejende sandsynligt, at en sådan person bruger en eller flere services fra den liste, der er på ovenstående PRISM-slide, hver eneste dag. Det kan være, at han afholder et Skype-møde eller gemmer noget i iCloud via et af sine Apple-produkter, og måske har han både en privat og en offentlig Facebook-profil, som han tilgår på daglig basis. Idet amerikanske services således anvendes, får det amerikanske NSA adgang til de herved generede data. Man kan da spørge, hvor ofte amerikanske politikere eller forretningsmænd gør brug af tilsvarende svenske onlineservices? Det må antages at være yderst sjældent – og nok nærmere aldrig (Hypponen, 2013). Det betyder i praksis, at NSA har et helt andet grundlag for dataindsamling, end man har i eksempelvis Sverige. Den amerikanske argumentation synes derved at være gennemhullet og savne berettigelse.

5.2. ETIKKENS BERETTIGELSE OG ANSVARLIG UDVIKLING AF TEKNOLOGI

I første del af indeværende kapitel blev udvalgte retskilder, der er med til at regulere databeskyttelse, fremstillet og diskuteret. Til trods for at der i EU er en omfattende juridisk ramme i forhold til databeskyttelse, vil det nu blive begrundet, hvorfor etik stadig har en berettigelse i forhold til disse regler. I afsnit 5.2.2., *Ansvarlig udvikling af teknologi i et EU-perspektiv*, vil jeg præsentere og diskutere, hvordan ansvarlig udvikling af teknologi anskues i EU.

5.2.1. ETIKKENS BERETTIGELSE I LYSET AF RETSKILDER OM DATABESKYTTELSE

Med afsæt i tre forskellige begrundelser vil det nu blive anskueliggjort, hvorfor etik har sin berettigelse i forhold de omfattende retskilder, der eksisterer på databeskyttelsesområdet – se hertil de følgende tre underafsnit. Den første begrundelse er ikke specifikt knyttet til databeskyttelse, og det diskuteres, hvordan etik er grundlaget for juridiske regler. Den efterfølgende begrundelse for etikkens berettigelse implicerer en ide om, at etik kan supplere juridiske regler. Dette argument vil blive eksemplificeret med Facebooks såkaldte "Datapolitik" og "Erklæring om rettigheder og ansvar". Den sidste begrundelse for at etik har sin berettigelse, knytter sig direkte til VSD og PbD, og det vil blive

demonstreret, at databeskyttelsesreguleringen i EU i sin nugældende form ikke i så høj grad sigter mod indflydelse på samme niveau som de metoder, som jeg i afhandlingens kapitel 8 behandler.

5.2.1.1. ETIK SOM FUNDAMENT FOR JURIDISKE REGLER

Etik – og etiske refleksioner om et givent emne – kan anses som værende fundamentet for juridiske regler. Dette argument tager afsæt i en grundlæggende ide om, at man, når man behandler et givent emne, må skelne mellem tre forskellige aspekter af en given problemstilling: Det tekniske/praktiske aspekt, det juridiske aspekt og det etiske aspekt (Øhrstøm, 2003, s. 24). Et eksempel på, hvor sondringen mellem det juridiske aspekt og det etiske aspekt optræder, er i forbindelse med Det Etiske Råds arbejde. Rådets arbejde er ikke at udforme lovgivning – derimod skal rådet sørge for at stille den fornødne etiske refleksion til rådighed for et folketing, der efterfølgende kan tage politiske beslutninger og producere egentlig lovgivning (Øhrstøm, 2003, s. 24). Det tekniske/praktiske aspekt i den situation består i, hvad der overhovedet er muligt at gøre.

Det må endvidere påpeges, at den teknologiske udvikling giver anledning til, at der kan opstå nye handlemuligheder, før der eksisterer retskilder til at "tage sig af" disse problemer. På tilsvarende vis kan gældende retskilder blive utilstrækkelige på grund af den teknologiske udvikling (Moor J. H., 1985, s. 266-267). Et eksempel herpå er databeskyttelsesdirektivet, der som nævnt er under modernisering. I sådanne tilfælde må overvejelser vedrørende det etiske og det tekniske/praktiske aspekt føre til udviklingen af nye eller modernisering af bestående retskilder.

5.2.1.2. ETIK SOM SUPPLEMENT TIL RETSKILDER

I dette afsnit vil der blive argumenteret for, at etik kan være anvendelig som et supplement til juridiske regler. Med afsæt i eksempler illustreres, at der kan være problemstillinger, der ikke nødvendigvis har en juridisk dimension, men som har en etisk dimension.

Databeskyttelsesdirektivet (og dermed også den danske persondatalov, der er afledt af databeskyttelsesdirektivet) har til formål at beskytte levende, identi-

ficerbare eller indirekte identificerbare personer. Der er i henhold til databeskyttelsesdirektivet adgang til at høste offentligt tilgængelige data online, så længe man sikrer sig, at man ikke kan identificere personer på baggrund af de høstede data. Sådanne offentligt tilgængelige data kan anvendes i den sammenhæng, som det nu ønskes.

Data fra sociale medier er her det oplagte eksempel på, at man kan høste data online og anvende disse. Som det vil blive eksemplificeret senere i afhandlingens i kapitel 7., *Dataveillance af big data som sikkerhedsteknologi*, så kan *tweets* fra Twitter scannes for udvalgte begreber eller sætningskonstruktioner med henblik på at afsløre ulovligheder – såkaldt *environmental scanning* (Brewster, et al., 2014a; Brewster, Polovina, Rankin, & Andrews, 2014b). Det er fuldt ud lovligt at anvende de nævnte former for indhentning af data – spørgsmålet er dog, om det er etisk forsvarligt.

Det forekommer at være overvejende sandsynligt, at når en person lægger data på et socialt medie, vil formålet dermed ikke være at producere data til politiet eller efterretningstjenester med henblik på at bidrage til opklaring af forbrydelser – og endnu mindre med henblik på selvinkriminering[140]. De personer, der skriver et *tweet* på Twitter eller skriver en statusopdatering på Facebook, forestiller sig formentlig ikke engang, at deres statusopdatering bliver scannet af en maskine for, om bestemte ord optræder.

Derimod forekommer det mere sandsynligt, at formålet med at gøre data tilgængelige online, er, at andre individer i en mere eller mindre afgrænset publikumskreds bestående af eksempelvis Facebook-venner eller følgere på Twitter skal kunne se disse. Den kontekst, som informationer ses i, ændres til en ny og anden kontekst, når informationerne scannes af eksempelvis en efterretningstjeneste.

[140] Gerstein har behandlet privathed i lyset af selvinkriminering. Det påpeges af Gerstein, at det er paradoksalt, at personer, der ikke er anklaget for en forbrydelse, kan pålægges at vidne i en sag. Det anses således for at have så stor samfundsmæssig betydning, at dette kan legitimere et tab af kontrol over information for den person, der vidner. Omvendt har den anklagede ikke pligt til at udtale sig (Gerstein, 1984b, s. 248) (Originalkilden blev publiceret første gang i 1970). Det er en interessant diskussion, som jeg dog ikke vil inddrage yderligere her, idet en sådan diskussion har en primært juridisk karakter.

Privathed problematiseres i ovenstående ud fra en kontekstuel forståelse af privathed (Moor J. H., 1997; Nissenbaum, 2010). Med afsæt i Nissenbaums *norms of flow or distribution*, der behandlet i foregående kapitel, er det ikke kun væsentligt, hvorvidt information er passende i en given kontekst – det er også væsentligt, hvordan information bevæger sig mellem kontekster (Nissenbaum, 2004, s. 140-141). I dette tilfælde flytter information sig fra én kontekst til én anden kontekst, hvilket kan betyde, at privathed kommer under pres.

Ideen om, at etik kan supplere databeskyttelse, kan yderligere udfoldes i forhold til globalisering. I kraft af internettet kan data nu bevæge sig mellem forskellige lande og kontinenter – og dermed også mellem forskellige jurisdiktioner. Som nævnt ovenfor er retskilder i EU og i USA vedrørende databeskyttelse særdeles forskellige til trods for, at de begge har FIP som grundlag. Der vil således være tale om, at samme faktiske forhold vil blive mødt med vidt forskellige juridiske regler afhængig af, om man er i EU eller i USA. I et sådant tilfælde vil den etiske ramme supplere den juridiske ramme. Postulatet er umiddelbart, at hvor den juridiske ramme er variabel, vil den etiske ramme i højere grad være konstant – i hvert fald i lande, der har samme normsystemer. Facebooks dataindsamling er et eksempel herpå, hvilket jeg nu vil udfolde.

Ved åbningen af en Facebook-profil samtykker man til en række vilkår, herunder en datapolitik og en række servicevilkår. Under overskriften "Hvordan bruger vi oplysningerne" beskriver Facebook indledningsvist, at de:

> "[...] bruger alle de oplysninger, vi har, til at tilbyde dig og understøtte vores tjenester. Det gør vi ved at:
>
> [...]
>
> Vi kan tilbyde vores tjenester, tilpasse indhold og foreslå dig forskelligt indhold ved at bruge disse oplysninger til at lære noget om, hvordan du bruger og interagerer med vores tjenester og de personer og ting, du er forbundet til og har interesse for på og uden for vores tjenester." (Facebook, 2015a).

Det fremgår, at Facebook bruger alle de oplysninger, Facebook har til rådighed, til blandt andet at tilpasse og foreslå indhold. Formuleringen: "[...] alle de

oplysninger, vi har [...]" henviser til det foregående afsnit i Facebooks datapolitik, *Hvilken type oplysninger indsamler vi?*. Deraf fremgår, at Facebook blandt andet indsamler data i forbindelse med kontooprettelse og ved brug af Facebook, herunder om kommunikation med andre brugere, lokation vedrørende uploadede billeder, informationer om den enkelte bruger oplyst af andre brugere, kontaktpersoners identitet, oplysninger om de enheder, som man tilgår Facebook med, styrestystem på disse enheder og en lang række andre informationer (Facebook, 2015a).

Det er dog ikke klart, hvad der mere præcist sker med en brugers data, når det kommer i hænderne på Facebook. Denne dataindsamling må antages at være uproblematisk ud fra et juridisk perspektiv, idet Facebook jo i forbindelse med kontooprettelsen varsler, at en sådan indsamling vil finde sted, men det kan overvejes, om den ud fra en etisk betragtning er rimelig.

Ovenstående citat fra Facebooks Datapolitik kan yderligere problematiseres i lyset af stk. 13, i Erklæring om rettigheder og ansvar, som man ligeledes samtykker til, når man åbner en Facebook-konto. Her fremgår det, at:

> "1. Du bliver informeret, før vi foretager ændringer i disse vilkår, og du får mulighed for at gennemse og kommentere de ændrede vilkår, før du fortsætter med at bruge vores tjenester.
>
> 2. Hvis vi foretager ændringer i politikker, retningslinjer eller andre vilkår, der er refereret til eller medtaget i denne erklæring, kan vi give meddelelse herom på siden for Facebooks sitestyring.
>
> 3. Din fortsatte brug af Facebook-tjenesterne efter ændringer i vores vilkår, politikker eller retningslinjer betragtes som din accept af vores ændrede vilkår, politikker eller retningslinjer." (Facebook, 2015b, s. stk 13).

Ovenstående citat hjemler adgang til, at Facebook kan ændre i Facebooks vilkår. Hvis en ændring gennemføres, bliver det meddelt brugeren – og fortsættes brugen af Facebook herefter, anses dette som et samtykke til de nye vilkår. Det fremgår ikke af det citerede, om der er nogle begrænsninger i, hvilke former for vilkårsændringer eller vilkår, der er tale om. Derved kan man som individ ikke vide, hvad man samtykker til – for man har netop samtykket til, at Facebook blot kan ændre dette. Igen opstår en problemstilling, der ud fra en

juridisk betragtning er uproblematisk. Også her finder jeg, at det er rimeligt at betragte situationen fra et etisk perspektiv og derfor overveje, om denne adgang til at foretage vilkårsændringer er rimelig over for brugerne.

Facebook er som allerede nævnt certificeret efter Safe Harbor-programmet mellem USA og EU. Denne certificering betyder blandt andet, at Facebook må overføre data til USA. Dette gør Facebook sine brugere opmærksomme på, idet Facebook skriver, at; "Du accepterer at have dine personlige oplysninger overført til og behandlet i USA." (Facebook, 2015b, s. 16). Disse data kan derfor principielt tilgås af eksempelvis amerikanske NSA i det øjeblik, de overføres til USA og dermed placeres på amerikanske servere. Denne flytning af data er uproblematisk rent juridisk, og Facebook kan i øvrigt hævde, at det eksplicit er anført i Facebooks vilkår, at data flyttes til USA. Spørgsmålet er derfor, om dataflytningen er etisk forsvarlig – har man som bruger en forventning om, at ens data flyttes til USA, når man åbner en Facebook-profil som borger i et EU-land?

Endnu en problemstilling kan illustrere, at en etisk refleksion kan supplere retskilder. I dag er det muligt at fremsætte forudsigelser ved at analysere *big data*. Data kan lagres billigt, og en af fordelene herved er netop, at indsamlet data senere kan anvendes i nye sammenhænge, hvormed data kan være med til at skabe ny værdi eller værdi i en helt ny sammenhæng. At skabe værdi på denne måde implicerer også, at man ikke altid kan og vil vide, hvad disse data på et senere tidspunkt skal anvendes til. Databeskyttelsesdirektivet stiller dog krav om, at man, når der indsamles data, skal indsamle sådant *til udtrykkeligt angivne og legitime formål*, jævnfør Direktiv 95/46/EF art. 6 stk. 1, b. Det kan således vise sig problematisk fra start at oplyse de personer, hvorom man indsamler data, hvad disse data indsamles med henblik på. Man kan dermed overveje, hvordan det overhovedet er muligt at samtykke til indsamling af data, som man endnu ikke ved, hvad skal anvendes til (Mayer-Schönberger & Cukier, 2013, s. 153).

Rent juridisk kan de nævnte eksempler forsvares, hvilket dog ikke nødvendigvis betyder, at de også kan forsvares etisk. At noget er tilgængeligt eller muligt

i juridisk forstand medfører ikke, at det også er *etisk forsvarligt.* Der kan således opstå situationer, hvor det ikke kun relevant at overveje, hvad man *må gøre* (juridiske begrænsninger) og *kan gøre* (tekniske muligheder og begrænsninger), men også, hvad man *bør gøre.*

5.2.1.3. Databeskyttelsesdirektiv 95/46/EF og værdibaserede designtilgange

Dette sidste argument knytter sig direkte til det nuværende databeskyttelsesdirektiv og til værdibaseret design. Designtilgangene vil først blive præsenteret i kapitel 8., *Realisering af værdier i design*. Her vil de kun blive introduceret i det omfang, der er nødvendigt for diskussion.

Databeskyttelsesdirektivet og designtilgangene sigter kun i ringe grad mod at behandle databeskyttelse på ensartede måder, hvorfor der er mulighed for, at de to delvist divergerende tilgange kan *supplere* hinanden.

VSD og PbD tager afsæt i en ide om, at en konkret teknologi kan udformes således, at en værdi som privathed kan realiseres heri. Privathed skal mere konkret behandles af designere, udviklere og ingeniører allerede i udviklingsfasen og dermed, før bestemte teknologiske beslutninger ikke kan ændres (Klitou, 2014, s. 267-268). At man realiserer sådanne værdier i forbindelse med udviklingen af teknologi betyder ikke, at brugen af teknologien nødvendigvis vil korrespondere hermed – det skal ikke læses som et teknologideterministisk perspektiv.

I modsætning hertil sigter databeskyttelsesdirektivet primært mod "den registeransvarlige" og "registerføreren". Ifølge databeskyttelsesdirektivet art. 2, litra d, er den registeransvarlige den "[...] fysiske eller juridiske person, offentlige myndighed, institution eller ethvert andet organ, der alene eller sammen med andre afgør, til hvilket formål og med hvilke hjælpemidler der må foretages behandling af personoplysninger; [...]" (Europa-parlamentet og rådets direktiv, 1995, art. 2, litra d) En såkaldt registerfører er i følge art. 2, litra e, den "[...] fysiske eller juridiske person, offentlige myndighed, institution eller ethvert andet organ, der behandler personoplysninger på den registeransvar-

liges vegne[...]" (Europa-parlamentet og rådets direktiv, 1995, art. 2, litra e). Af art. 17 om behandlingssikkerhed fremgår det, at:

> "Artikel 17
>
> Behandlingssikkerhed
>
> 1. Medlemsstaterne fastsætter bestemmelser om, at den registeransvarlige skal iværksætte de fornødne tekniske og organisatoriske foranstaltninger til at beskytte personoplysninger mod hændelig eller ulovlig tilintetgørelse, mod hændeligt tab, mod forringelse, ubeføjet udbredelse eller ikke-autoriseret adgang, navnlig hvis behandlingen omfatter fremsendelser af oplysninger i et net, samt mod enhver anden form for ulovlig behandling.
>
> Disse foranstaltninger skal under hensyn til det aktuelle tekniske niveau og de omkostninger, som er forbundet med deres iværksættelse, tilvejebringe et tilstrækkeligt sikkerhedsniveau i forhold til de risici, som behandlingen indebærer, og arten af de oplysninger, som skal beskyttes.
>
> 2. Medlemsstaterne fastsætter bestemmelser om, at den registeransvarlige, hvis oplysninger behandles for dennes regning, skal vælge en registerfører, som frembyder den fornødne garanti med hensyn til de tekniske sikkerhedsforanstaltninger og organisatoriske foranstaltninger, der skal træffes, og skal påse, at disse foranstaltninger overholdes." (Europa-parlamentet og rådets direktiv, 1995, art. 17).

Det er den registeransvarlige, der skal forestå tekniske og organisatoriske foranstaltninger med henblik på sikker behandling af personlige oplysninger. Det betyder også, at det ikke er i forbindelse med udvikling af en given teknologi, at der foreligger et krav om beskyttelse – det er i forbindelse med anvendelsen af data, at den registeransvarlige skal sikre data.

Af sagsfremstilling (recital) 46 i direktiv 95/46/EF fremgår det dog også, at:

> "(46) beskyttelsen af de registreredes rettigheder og frihedsrettigheder i forbindelse med behandling af personoplysninger forudsætter, at der træffes de fornødne tekniske og organisatoriske foranstaltninger både under selve udformningen og under iværksættelsen af en behandling, navnlig for at varetage sikkerheden og derved forhindre enhver form for ubeføjet behandling; det påhviler medlemsstaterne at sørge for, at de registeransvarlige overholder disse foranstaltninger; disse foranstaltninger skal under hensyn til det aktuelle tekniske niveau og de omkostninger, som

> er forbundet med deres iværksættelse, tilvejebringe et tilstrækkeligt sikkerhedsniveau i forhold til de risici, som behandlingen indebærer, og arten af de oplysninger, der skal beskyttes;" (Europa-parlamentet og rådets direktiv, 1995, sagsfremstilling 46).

Hermed er således et eksempel på, at en grundlæggende ide om, at man allerede under "udformningen og iværksættelsen" kan beskytte den registreredes rettigheder. Allerede i 2009 bemærkede den såkaldte Article 9 Working Party (ARTICLE 29 Data Protection Working Party, 2009), at databeskyttelsesdirektivet i nogen grad har peget mod Privacy by Design-principper, hvor man allerede tager privathed i betragtning i forbindelse med selve udviklingen af teknologi. Dette findes dog ikke at have været tilstrækkeligt, idet Article 29 Working Party påpeger, at:

> "This principle (privacy by design, red.) should be binding for technology designers and producers as well as for data controllers who have to decide on the acquisition and use of ICT. They should be obliged to take technological data protection into account already at the planning stage of information-technological procedures and systems." (ARTICLE 29 Data Protection Working Party, 2009, s. 13).

Direktiv 2002/58/EF om elektronisk kommunikation fremsætter også ideen om, at selve det tekniske udstyr skal fremstilles således, at det fordrer beskyttelse af information:

> "Hvor der er behov herfor, kan der vedtages foranstaltninger for at sikre, at terminaludstyr fremstilles på en måde, der er forenelig med brugernes ret til at beskytte og kontrollere anvendelsen af deres personoplysninger [...]." (Europa-parlamentets og rådets direktiv, 2002, § 14, stk 3).

Art. 14, stk. 3, udgør en undtagelse til, at man i EU sigter mod registerfører og registeransvarlig i databeskyttelseslovgivning. I ovenstående nævnes netop, at terminaludstyr skal fremstilles således, at brugerne kan beskytte og kontrollere personoplysninger. Desuden sigter databeskyttelse i EU på en snæver forståelse af databeskyttelse, hvor dette primært forstås som datasikkerhed (Klitou, 2014, s. 274). Netop at PbD og VSD ikke har samme tilgang som det nuværende databeskyttelsesdirektiv betyder, at metoderne kan opfattes som et bidrag til og en mulighed for udvikling af ansvarlig teknologi.

5.2.2. ANSVARLIG UDVIKLING AF TEKNOLOGI I ET EU-PERSPEKTIV

At udvikling og forskning sker på en ansvarlig måde, er et fokusområde i EU, idet forskning og innovation anses for at være grundpiller i EU's fremgang og vækst. Dette bliver også tydeligt i en rapport fra Europa Kommissionen fra 2013 om såkaldt "Responsible Research and Innovation" (herefter blot RRI) (European Commission, 2013). I rapporten omtales en RRI-strategi, der kan sammenlignes med virksomheders arbejde med Corporate Social Resposibility-strategier (også kendt i daglig tale som CSR-strategier). Corporate Social Responsibility kan defineres som: "[...] en virksomheds frivillige inddragelse af sociale og miljømæssige hensyn i dens forretningsaktiviteter." (Den Store Danske).

RRI er et paraplybegreb, der i rapporten er defineret som:

> "[...] the comprehensive approach of proceeding in research and innovation in ways that allow all stakeholders that are involved in the processes of research and innovation at an early stage. (A) to obtain relevant knowledge on the consequences of the outcomes of their actions and on the range of options open to them and (B) to effectively evaluate both outcomes and options in terms of societal needs and moral values and (C) to use these considerations (under A and B) as functional requirements for design and development of new research, products and services." (European Commission, 2013, s. 3).

RRI og dermed også værdibaseret design må nødvendigvis tage afsæt i grundlæggende antagelser om, at det er meningsfuldt at tale om etiske spørgsmål med henblik på til en vis grad at opnå etisk konsensus, og ikke mindst at dette rent faktisk også er muligt. Implicit afvises hermed også etisk intuitionisme, hvor etikken regnes for en tavs kompetence – et synspunkt, der forsvares af eksempelvis K. E. Løgstrup. Ydermere tages der også afstand fra emotivistiske ideer, hvormed etikken reduceres til udsagn af følelsesmæssigt karakter, eller med andre ord blot er udtryk for ønsker (Ayer, 1990, s. 104-126)[141]. Ayer skriver, at:

> "[...] in everycase in which one would commonly be said to be making an ethical judgement, the function of the relevant ethical

[141] Originalkilden blev publiceret første gang i 1936.

> word is purely 'emotive'. It is used to express feeling about certain objects, but not to make any assertion about them." (Ayer, 1990, s. 111).

Tilgangen til etiske spørgsmål, hvor fundamentet er mere rationelt, er her ligeledes grundlaget for nærværende afhandling. I fald man har overbevisninger omkring etikken, som noget vi ikke kan diskutere på mere rationelle præmisser, ville nærværende afhandling ikke have nogen berettigelse.

I RRI-rapporten demonstreres endvidere nødvendigheden af at foretage etiske overvejelser forud for design, idet dette vurderes at kunne højne de samlede samfundsmæssige og individrelaterede fordele. Ydermere slås det også fast, at der findes empirisk belæg for, at dette er hensigtsmæssigt i kraft af udviklingsprojekter, hvor de etiske overvejelser indledningsvist ikke er blevet foretaget i tilfredsstillende grad, hvorfor de samfundsmæssige og individrelaterede konsekvenser af en given innovation har været af negativ karakter (European Commission, 2013, s. 3). Forskning og innovation med fokus på at øge de samfundsmæssige fordele er ligeledes en del af en række mere overordnede politikker og strategier i EU (eksempelvis Horizon 2020). Desuden lægges der i rapporten vægt på, at: "[...] it is widely acknowledged that there is a need to better incorporate ethical concerns in research and innovation." (European Commission, 2013, s. 11). Dertil skal det nævnes, at sikkerhedsteknologi eksplicit nævnes i RRI-rapporten, som en af de typer af teknologier, der er omstridte, da der i forbindelse med udvikling heraf ikke er taget tilstrækkelig højde for de etiske anliggender og samfundsmæssige behov (European Commission, 2013, s. 13).

Endvidere er det klart, at et forsknings- og innovationsprojekt, der ender med at gå til grunde som følge af eksempelvis manglende etiske vurderinger i den indledende fase, vil medføre økonomiske tab. I stedet for at spilde økonomiske ressourcer kan disse problemer afværges ved en proaktiv tilgang til design. Samtidigt hermed skal det bemærkes, at det omvendte (at tage etiske overvejelser i betragtning proaktivt i en udviklingsproces) ifølge EU-rapporten kan give betydelige økonomiske fordele (European Commission, 2013, s. 14). Der nævnes i rapporten konkrete eksempler på, at privathed ikke har været taget i

betragtning i udgangspunktet af et udviklingsprojekt, hvorfor man efterfølgende har set sig nødsaget til at droppe dette med store økonomiske tab til følge. For eksempel findes såkaldte "smart energy meters" i Holland, hvilket har været en del af en mere bred EU-strategi. Efter flere års forskning og udvikling af dette område måtte man droppe implementeringen af "smart energy meters", da man mente, at der var signifikante problemer i forhold til privathed (European Commission, 2013, s. 59). Med kendskab til en husholdnings energiforbrug kan man få en indgående viden om en families daglige gøren og laden. I rapporten gøres det klart, at såfremt man havde taget disse privathedsrelaterede overvejelser med indledningsvist i udvikling af "smart energy meters", kunne man have undgået den beskrevne situation (European Commission, 2013, s. 59).

Projekter, der går i vasken, fordi man "glemmer" at tænke på privathed i en designproces, er også med til at understøtte Wang og Kobsas bemærkning[142] om, at det er svært at "retro-fitte" et system og gøre dette mere privathedsvenligt, hvis dette ikke er taget i betragtning indledningsvist (Wang & Kobsa, 2008, s. 18). Det er med andre ord ønskværdigt, at en teknologi eksempelvis et stykke software designes med blik for ønskede værdier i stedet for, at disse skal ændres efter, at softwaren er blevet en del af en organisation eller et socialt system (Friedman & Kahn, 2003, s. 1195). Af samme grund påpeger Friedman et al også, at det er nødvendigt, at man anlægger en proaktiv tilgang til menneskelige værdier, etik og design (Friedman & Kahn, 2003, s. 1195).

Der er ifølge EU-rapporten ikke nogle kohærente guidelines, der beskriver, hvordan RRI føjes til forsknings- og udviklingsprocesser. Det slås endvidere i RRI-rapporten fast, at der er et øget fokus på ansvarlig forskning og innovation, men at dette ikke rutinemæssigt bliver taget i betragtning i udviklingsprojekter. Denne manglende fokus på RRI kan også ses implicit i den akademiske

[142] Citatet, der også findes tidligere i afhandlingen, har følgende ordlyd: "Privacy needs to be treated as a first-class requirement from the early onset in the design of an information system since, like for security and usability, it is extremely difficult if not impossible to "retrofit" a completed system to make it more privacy-friendly." (Wang & Kobsa, 2008, s. 18)

verden, idet der ikke er mange videnskabelige *high impact journals*, der sigter mod sådanne emner (European Commission, 2013, s. 17).

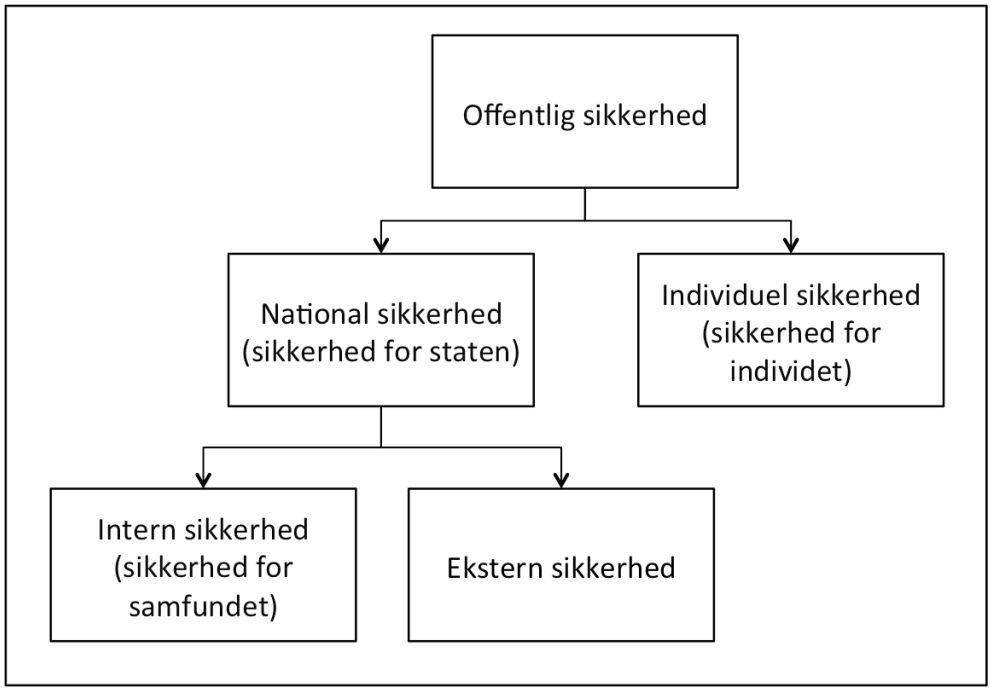
Værdibaseret design (herunder mere specifikt VSD) er blevet sat i forbindelse med RRI (Timmermans & Mittelstadt, 2014, s. 3) og siges i den forbindelse at kunne få en rolle som den mere konkrete strategi til at løfte RRI-strategien i praksis i projekter. Hvorvidt disse konkrete tilgange er hensigtsmæssige i forhold til sikkerhedsteknologi, vil blive diskuteret i afhandlingen. Ligeledes nævnes Privacy by Design som strategi også eksplicit i RRI-rapporten som en måde at implementere privathed i IKT-udvikling samtidigt med, at de ønskede funktioner stadig er til stede.

Ofte bliver den etiske tænkning anset for at være en begrænsende faktor eller ligefrem en hæmsko for forskning, udvikling og innovation (van den Hoven, Lokhorst, & Poel, 2011, s. 143-144). Et typisk narrativ, der præsenteres i den forbindelse, tilsiger, at det ud fra en økonomisk betragtning ikke er hensigtsmæssigt at "holde på" retten til privathed, da dette blot vil begrænse udviklingen for virksomheder, der arbejder med sikkerhedsteknologi. Vi takker dermed også implicit nej til økonomisk fremdrift og udvikling (European Commission, 2014a, s. 80). Denne fremstilling af manglende mulighed for økonomisk fremdrift kan synes problematisk. Der kan omvendt argumenteres for, at etisk tænkning kan være en *driver* for nye forskningsområder og en måde, hvorpå der kan skabes jobs og velfærd. Dermed synes det rimeligt at argumentere for, at hvis der er jobs i fremstilling af sikkerhedsteknologi, så må der nødvendigvis også være jobs i ansvarlig fremstilling af sikkerhedsteknologi. Samtidigt vil man med afsæt i en ansvarlig tilgang undgå forkert allokering af økonomiske ressourcer ved udvikling af ny teknologi som eksemplificeret ovenfor. Fordelene ved at satse på RRI og dermed VSD og PbD synes således at være flere.

6. OFFENTLIG SIKKERHED

6. OFFENTLIG SIKKERHED

I dette kapitel belyses offentlig sikkerhed. Offentlig sikkerhed optræder i afhandlingen som et paraplybegreb, der dækker over sikkerhed for en stat såvel som sikkerhed for individer. Sikkerheden for en stat kan være sikkerhed i forhold til både interne og eksterne trusler.[143] Hvad angår de interne trusler mod en stat, kan man igen skelne mellem trusler kommende fra staten og trusler kommende fra andre individer.[144] Nedenstående figur 2 kan illustrere sammenhængene i sikkerhedsbegrebet, som jeg opererer med i afhandlingen.



Figur 2: Oversigt over sikkerhedsbegrebet i afhandlingen

Betegnelsen "offentlig sikkerhed" anvendes i afhandlingen, idet begrebet jævnligt bruges til at henvise til sikkerhed i forhold til terror og organiseret

[143] Mexico kan her tjene som et eksempel til at illustrere, hvorfor denne sondring imellem statens interne og eksterne sikkerhed er hensigtsmæssig. Den interne sikkerhed i Mexico er ifølge en rapport fra RAND Corporation (Schaefer, Bahney, & Riley, 2009) blevet forringet over de seneste år. Denne forringelse skyldes blandt andet organiseret kriminalitet, herunder narko-relateret kriminalitet og korruption. Mexico er dog ikke i krig med andre nationer, hvorfor den eksterne sikkerhed ikke er under pres.

[144] Hobbes har denne sondring, hvilket jeg vender tilbage til senere i dette afsnit.

kriminalitet (Aquilina, 2010, s. 131). Det er netop disse former for trusler, som de sikkerhedsteknologier, jeg belyser i afhandlingen, sigter i mod. Derudover er begrebet brugbart i forhold til at indfange en stat (internt og eksternt) og individer som referenter for sikkerhed, hvilket er i modsætning til en betegnelse som national sikkerhed. National sikkerhed udpeger i højere grad en stat alene som referent for sikkerhed (Owen, 2004, s. 16).

Det er også væsentligt at bemærke, at en trussel mod offentlig sikkerhed ikke nødvendigvis er en trussel mod *enten* statens sikkerhed eller individets sikkerhed. Terror er det oplagte eksempel på, at en trussel kan berøre såvel en stats interne sikkerhed som individers sikkerhed. Dette er også grunden til, at jeg senere vil argumentere for, at en vurdering af sikkerhed, der kun tager statens sikkerhed i betragtning, ikke er tilstrækkelig.

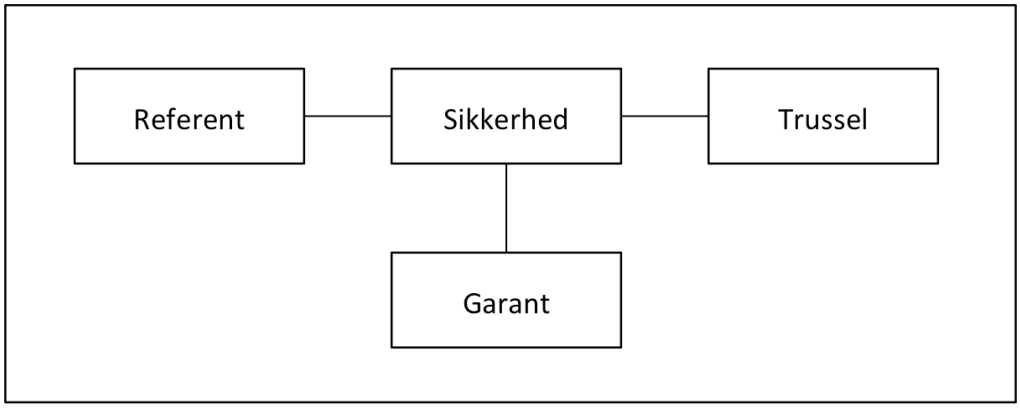
I indeværende kapitel vil der grundlæggende blive argumenteret for, at staten er mere end blot summen af individer. Dette er også en grundlæggende antagelse i hele afhandlingen, idet staten er i stand til sætte individers privathed under pres – det kan trods alt kun lade sig gøre, hvis staten i ontologisk forstand adskiller sig fra individerne.

Nærværende kapitel falder i to hoveddele.

I kapitlets første del, 6.1., *Offentlig sikkerhed og relationen mellem stat og individ,* diskuteres det indledningsvist, hvad der udpeges med begreberne 'sikker' og 'sikkerhed'. Dernæst diskuteres og præciseres det, hvad der i afhandlingen forstås ved offentlig sikkerhed, og hvem der er referent for denne sikkerhed. Med referenten for sikkerhed henvises til den, der er sikker eller er i sikkerhed. Referenten for denne sikkerhed kan i afhandlingen være staten (internt eller eksternt) såvel som individer i staten. Sikkerhed forstås med andre ord med afsæt i en tertiær relation, hvor der er et subjekt (referenten: Individ eller staten), der garanteres sikkerhed af et andet subjekt, en stat eller et individ.

Den anden del, 6.2., *Sikkerhedsbegrebet i udvalgte retskilder,* behandler en række udvalgte retskilder, hvori sikkerhed spiller en betydningsfuld rolle. Med afsæt i samme retskilder diskuteres perspektiver for sikkerhed.

Indledningsvist vil jeg knytte en kommentar til sikkerhedsbegrebet mere generelt. Den tærtiere relation, som jeg omtalte i ovenstående, er visualiseret figur 3: Visualisering af tertiær relation.



Figur 3: Visualisering af tertiær relation

Relationen, som er visualiseret i ovenstående figur, giver mulighed for otte kombinationer. Disse er fremstillet i nedenstående tabel 1, *Kombinationsmuligheder på baggrund af relation,* hvor der også er givet et eksempel på de enkelte mulige kombinationsmuligheder. Som det fremgår af tabellen, er ikke alle kombinationer realistiske (se kombination B og F). Kombinationerne D og H er ikke urealistiske, men dog irrelevante, idet afhandlingen tager afsæt i, at staten er garant for sikkerheden.

Kombination	Garant for sikkerhed	Referent for sikkerhed	Trussel	Eksempel på relation
A	Stat	Stat	Stat	Et stort land beskytter et mindre land mod trussel fra tredje stat. En stats forsvar beskytter landet mod trusler fra andre lande.
B	Individ	Stat	Stat	-
C	Stat	individ	Stat	Menneskerettigheder har blandt andet til formål at sikre individer mod overgreb fra staten.
D	Individ	Individ	Stat	Ikke relevant[145]
E	Stat	Stat	Individ	Statens efterretningstjeneste beskytter staten mod trusler fra terrorist.
F	Individ	Stat	Individ	-
G	Stat	Individ	Individ	Politiet beskytter individer mod overgreb fra andre individer.
H	Individ	Individ	Individ	Ikke relevant[146]

Tabel 1: Kombinationsmuligheder på baggrund af relation

[145] Man kan forestille sig en situation, hvor et statsligt organ fratager et individ nogle økonomiske midler, som er væsentlige for individets levevilkår. Den forurettede beskyttes af et person, der er særligt ressourcestræk og derfor kan hjælpe den forurettede i "kampen mod" myndighederne.

[146] Forældre beskytter børn mod overgreb fra andre personer.

Det fremgår af tabel 1, at i de tilfælde, hvor et individ er garant for sikkerheden (B, D, F, H), er der tale om en kombination, der enten er irrelevant eller urealistisk.

Hvem der er opfattet som en mulig referent for sikkerhed, kan siges at have forandret sig over tid. Der kan således observeres et skift fra en traditionel forståelse, hvor staten er referent, til en bredere sikkerhedsforståelse, der hviler på et liberalt fundament, der også har individet som referent (Liotta, 2002, s. 473-475). Den traditionelle forståelse af sikkerhed har primært omhandlet statens evne til at modgå eksterne trusler og har således også været formuleret med et militaristisk og geografisk orienteret afsæt. Den traditionelle, stats-orienterede opfattelse af sikkerhed, der var særligt dominerende omkring slutningen af den kolde krig, byggede på en antagelse om, at såfremt staten var i sikkerhed, så var individerne i staten det ligeledes (Owen, 2004, s. 16).

Den statsorienterede tilgang til sikkerhed anses ikke længere for tilstrækkelig, hvorfor man siden midten af 1990'erne i højere grad har haft blik for individet som referent for sikkerhed. Det er i forbindelse hermed væsentligt at påpege, at det i afhandlingen ikke opfattes således, at det mere individ-orienterede sikkerheds-paradigme har "overtaget" den nationale sikkerhedsprioritet. Derimod anses såvel stat som individ for at være relevante referenter for sikkerhed.

I kapitlets første del præsenteres en diskussion af relationen mellem stat og individer i forhold til sikkerhed. Denne diskussion er nødvendig, idet det perspektiv, der anlægges på relationen mellem stat og individ, har signifikant betydning for, hvor det moralske ansvar er placeret, og hvem der med andre ord er den moralske agent. Med afsæt i blandt andre Thomas Hobbes (2001)[147] og David Hume (1999)[148], vil forholdet mellem stat og individ blive diskuteret. Netop opretholdelse af sikkerhed er for Hobbes begrundelsen for,

[147] Originalkilden blev publiceret første gang i 1651.

[148] Originalkilden blev publiceret første gang i 1740.

at vi nødvendigvis skal skabe en stat – sikkerhed legitimerer med andre ord statsmagten. Skaber vi ikke en stat, vil mennesker som egoistiske dyr blot ende i krig (Hobbes, 2001, s. 57). I modsætning til Hobbes mener Hume, at en gruppe af individer finder sammen for at skabe sikkerhed, hvilket også implicerer, at individerne ikke nødvendigvis er fjender indtil det punkt, hvor statsmagten introduceres (Hume, 1999, s. 330).

6.1. OFFENTLIG SIKKERHED OG RELATIONEN MELLEM STAT OG INDIVID

I nærværende afsnit vil offentlig sikkerhed blive diskuteret, og en forståelse heraf vil blive præciseret. Indledningsvist vil dette ske ved at belyse betydningen af adjektivet "sikker" og substantivet "sikkerhed". Herved demonstreres det, at sikker og sikkerhed ikke er entydige begreber, men at der er forskellige aspekter af sikkerhed. Disse forskellige betydninger hænger dog sammen i systematisk forstand – de hører til det samme domæne med andre ord. Efterfølgende diskuteres perspektiver på relationen mellem stat og individ. I forlængelse heraf diskuteres den udvikling i forståelsen af sikkerhed, der er sket, fra blot at være orienteret mod nationen til også at inddrage individet.

6.1.1. SIKKERHEDENS SEMANTIK

Adjektivet "sikker" kommer af det latinske *securus* (Lund, 2007). Det latinske "se" kan betyde "uden", og "cura" kan betyde "bekymring" (Hastrup, 1976). Ifølge Den Danske Ordbog betyder sikker blandt andet: "[...] som ikke frembryder eller indebærer fare eller risiko for uønskede eller ubehagelige situationer." (ordnet.dk, sikker).[149] Hvorvidt "sikker" i afhandlingens kontekst kan siges at udpege det "at være uden bekymring" eller fraværet af en ubehagelig situation, kan problematiseres. Man kan med andre tale om forskellige aspekter af sikkerhed: Sikkerhed som fri for fare og sikkerhed som fri for bekymring. Netop denne betydningsmæssige forskel kan siges at være i direkte forbindelse med sondringen mellem sikkerhed for staten og sikkerhed for indivi-

[149] "Sikker" kan også anvendes i andre sammenhænge. Eksempler herpå er at være sikker i sin sag, sikkerhed i økonomisk forstand, at være sikker i noget i betydningen at være dygtig (ordnet.dk, sikker).

det. Kritikken af ideen om sikkerhed for individet lyder, at dette leder til et perspektiv på sikkerhed som fri fra bekymring. Sikker kan således konnotere en forståelse af, at der hermed er tale om at have det komfortabelt. Problemstillingen, der omhandler forståelsen af "at være sikker", vil blive udfoldet yderligere i næste afsnit.

Substantivet sikkerhed kommer af det latinske *securitas* (Lund, 2007). Det danske ord sikkerhed kan ifølge Ordbogen.com dække over begge de engelske begreber "security" og "safety" (ordbogen.com, sikkerhed). Ifølge Oxford Dictionaries udpeger "security": "The state of being free from danger or threat." (oxforddictionaries.com, security), mens "safety" betyder: "The condition of being protected from or unlikely to cause danger, risk, or injury." (oxforddictionaries.com, safety). Heraf fremgår det, at det engelske "security" udpeger en tilstand, et individ kan befinde sig i. I modsætning hertil refererer "safety" til beskyttelse mod en fare. Ifølge www.ordnet.dk er betydningen af det danske ord sikkerhed imidlertid en: "[...] tilstand hvor man er uden for fare eller fri for en uønsket eller ubehagelig situation" (ordbogen.com, sikkerhed). Dette stemmer umiddelbart bedst overens med den føromtalte definition fra Oxford Dictionaries af "security", idet der i begge tilfælde er tale om *en tilstand.*

På tysk anvendes ligesom på dansk kun ét begreb, "Sicherheit", der dækker over såvel "safety" som "security" (van Lieshout, Friedewald, Wright, & Gutwirth, 2013, s. 122). Kigger man på betydningen af begreberne "sikkerhed", "security" og "safety", synes der at være dækning for at hævde, at sikkerhed helt basalt handler om ikke at være i fare. Dette stemmer endvidere overens med van Kempen, der har påpeget, at sikkerhed kan beskrives som: "[...] freedom from such phenomena as threat, danger, vulnerability, menace, force and attack." (van Kempen, 2013, s. 2). Denne definition tager afsæt i samme ide, som udtrykkes i en rapport fra EU, hvori det påpeges, at sikkerhed i dag ofte forstås som: "[...] to a condition of safety, of being protected, free from danger [...]" (European Commission, 2014a, s. 61). Hvis man anser van Kempens brede definition af sikkerhed som et kriterium for tilstedeværelse af sikkerhed,

rejser der sig dog andre spørgsmål: Sikkerhed for hvem? Og i forlængelse heraf også hvem der skal facilitere denne sikkerhed?

6.1.2. SIKKERHED FOR HVEM OG STATENS LEGITIMITET

Offentlig sikkerhed opfattes som tidligere nævnt som et paraplybegreb, og dermed har offentlig sikkerhed også to referenter, nemlig stat og individ. Offentlig sikkerhed består således af national sikkerhed[150], der udpeger en stats evne til at forsvare sig imod udefrakommende trusler og til at beskytte statens integritet. Dermed falder en stats interne sikkerhed også ind under dette begreb – samfundets sikkerhed med andre ord. Ydermere inkluderer offentlig sikkerhed det, som man ofte ser benævnt "human security". I denne afhandling vil jeg anvende begrebet individuel sikkerhed. Denne form for sikkerhed dækker over sikkerhed for de enkelte individer (Liotta, 2002, s. 475).

Sikkerhed kan opfattes som en grundlæggende, motiverende årsag til statsdannelsen (European Commission, 2014a, s. 61-63). Hvordan relationen mellem stat og individer ideelt set skal udformes, er der særdeles divergerende ideer om, og problemstillingen har længe været flittigt diskuteret indenfor den politiske filosofiske tradition (Owen, 2004, s. 15-16). En måde at tilgå spørgsmål om relationen mellem stat og individ er som en social kontrakt. En social kontraktteori handler grundlæggende om den kontrakt, der indgås mellem mindst to subjekter om at udveksle goder eller servicer. Ydermere skal en social kontraktteori redegøre for, hvor meget magt en stat skal have efter etableringen heraf. Udgangspunktet for social kontraktteori er dog at besvare, hvad der eksisterede, før man etablerede en statsmagt, hvilket kan legitimere behovet for statsmagten.

Et eksempel på en kontraktteoretiker er Thomas Hobbes (1588-1679), der har påpeget nødvendigheden af en absolutistisk statsmagt, der kan retfærdiggøres ved fraværet af naturtilstanden. Den absolutte statsmagt implicerer også, at individet skal opgive samtlige rettigheder (Hobbes, 2001). Hobbes perspektiv inkluderer tillige det synspunkt, at såfremt staten er sikker, så er indi-

[150] På engelsk anvendes blandt andre begreberne "national security", "security of the state" og "state security".

vider i denne stat det også – ideen centrerer sig således om interne forhold i staten (Hobbes, 2001, s. 57). Jeg vender tilbage til Hobbes ide senere i nærværende afsnit.

En anden teoretisk tradition, der også beskæftiger sig med statens konstruktion, er den utilitaristiske. Ideen er her, at sikkerhed er en nødvendig betingelse for frihed (Zedner, 2009, s. 27). Jeremy Bentham (2007) forsvarede den klassiske utilitarisme, der gør gældende, at staten skal struktureres omkring mest mulig nytte til flest mulige – det såkaldte *The Principle of Utility,* der har følgende ordlyd:

> "NATURE has placed mankind under the governance of two sovereign masters, pain and pleasure. It is for them alone to point out what we ought to do, as well as to determine what we shall do." (Bentham, 2007, s. 1).

Det eneste, der ifølge utilitarismen er godt i sig selv, er nydelse, og det eneste vi skal undgå, er smerte (Bentham, 2007, s. 102). Formålet med nytteprincippet er et princip: "[...] which approves or disapproves of every action whatsoever [...]" (Bentham, 2007, s. 1-2). Nytteprincippet kan anvendes til at legitimere love, som staten vedtager, og handlinger, som staten udfører, hvis disse opfylder betingelsen i nytteprincippet om at give mest mulig nytte til flest mulige. Den praktiske implikation heraf er, at statsmagten således også får muligheden for at "sælge" nogle for flertallets gode.

Hos Hobbes er det som nævnt staten, der er "det primære" og dermed også mere end blot summen af individer. Det implicerer, at staten har (moralsk) autoritet overfor individet. Denne relation fremgår også af illustrationen på billede 9, der er den øverste del af forsidebilledet på Hobbes værk "Leviathan" (Hobbes, 2001). Leviathan også er navnet på et havuhyre, der optræder i det gamle testamente. Billede 9 forestiller den absolutte statsmagt, Suværenen, hvis krop udgøres af individerne i en stat. Disse individer har ingen ret til at modgå statsmagten.

Billede 9: Del af forsidebillede fra bogen Letivathan (Hobbes, 2008) .

Det følger af Hobbes ide om forholdet mellem stat og individ, at det er staten, der skal sørge for individets sikkerhed. Hvis staten ikke sørger for sikkerheden, vil det enkelte individ være i en naturtilstand. Hos Hobbes er naturtilstanden et analytisk begreb, der således ikke må forveksles med en egentlig tidsperiode. I naturtilstanden har det frie individ ikke bare rum, men også ret til at opføre sig som et egoistisk dyr og har dermed kun den sikkerhed, som egen styrke kan give (Hobbes, 2001, s. 57). Individer, der befinder sig i naturtilstanden, vil således befinde sig i en konstant kamp for at overleve.

Bevægelsen fra naturtilstanden til en civiliseret stat, hvor fare og usikkerhed ikke eksisterer på samme måde, implicerer dog ifølge Hobbes, at individer skal opgive rettigheder til staten, for at det er muligt for staten at sikre dem. Hobbes beskriver dette i sit værk Leaviathan således:

> "Hereby it is manifest that during the time men live without a common power to keep them all in awe, they are in that condition which is called war; and such war is of every man against every man. [...]

> Whatsoever therefore is consequent to a time of war, where every man is enemy to every man, the same consequent to the time wherein men live without other security then what their own strength and their own invention shall furnish them withal. In such condition there it no place for industry, beaches the fruit thereof is uncertain: and consequently no culture of the earth; no navigation, nor use of the commodities that may be imported by sea; no commodious building; no instruments of moving and removing such things as require much force; no knowledge of the face of the earth; no account of time; no arts; no letters; no society; and which is worst of all, continual fear, and danger of violent death; and the life of man, solitary, poor, nasty, brutish, and short." (Hobbes, 2001, s. 57).

Individet har ifølge Hobbes et naturligt ønske om ikke at leve i usikkerhed, hvorved Hobbes kan retfærdiggøre ideen om en absolutistisk statsmagt. Ifølge Hobbes skal alle individer overdrage rettigheder til staten. Dette forhold har Hobbes beskrevet med ordene:

> "I authorise and give my right to governing myself to this man, or to this assembly of man, on this condition; that thou give up, thy right to him, and authorise all his action in like manner. This done, the multitude so united in one person is called a COMMONWEALTH; in Latin, CIVITAS." (Hobbes, 2001, s. 78-79).

Hobbes benævner den absolutte statsmagt Commonwealth, hvilket kan oversættes til dansk med Suværenen (Hobbes, 2008, s. 175). Hermed er det hierarki, der er i en stat, tydeligt illustreret sprogligt. Undersåtternes overdragelse af magt og rettigheder til Suverænen betyder, at der nu kan opretholdes fred og sikkerhed:

> "The only way to erect such a common power, as may be able to defend them from the invasion of foreigners, and the injuries of one another, and thereby to secure them in such sort as that by their own industry and by the fruits of the earth they may nourish themselves and live contentedly, is to confer all their power and strength upon one man, or upon assembly of men, that may reduce all their wills, by plurality of voices, unto one will: which is as much as to say, to appoint one man, or assembly of men, to bear their person; and every on to own and acknowledge himself to be author of whatsoever he that so beareth their person shall act, or cause to be acted, in those things which concern the common peace and safety; and therein to submit their wills, every one to

> his will, and their judgement to his judgement." (Hobbes, 2001, s. 78).

Den sondring, som jeg i afhandlingen opererer med mellem sikkerhed for en stat og sikkerhed for et individ, optræder eksplicit i ovenstående citat. Hobbes påpeger, at man skal sikre sig i mod invasioner fra fremmede – der er her tale om statens sikkerhed i forhold til andre stater. Vi skal sikre staten mod aggressioner udefra. Desuden skal individer beskyttes mod hinanden. Her er der tale om individets sikkerhed.

Dog opereres der i afhandlingen også med den grundlæggende antagelse, at staten kan true individet. Hvis man anlægger et perspektiv på statsmagten, der som Hobbes perspektiv er absolut, vil det ikke være meningsfuldt at diskutere individers frihedsrettigheder, herunder privathed. Individer afgiver rettigheder til statsmagten, og der indgås en kontrakt. I bytte for afgivelse af rettigheder får individer sikkerhed (Hobbes, 2001, s. 60-61). Det er dermed også klart, at Hobbes perspektiv må afvises.

I modsætning til Hobbes mener liberalismens grundlægger og fortaler for en minimalstat, John Locke (1632-1704), at statens opgave er at sikre individets frihed og lighed (Locke, 2003)[151]. Individet er ifølge Locke frit og skal heller ikke – i modsætning til Hobbes teori - opgive sine rettigheder til staten. Statens opgave er at beskytte individets naturlige rettigheder. Lockes ide er, at en række love baseret på fornuft allerede eksisterer før oprettelsen af statsmagten, men disse er dog usikre, hvorfor det er meningsfuldt at sikre dem gennem en social kontrakt (Locke, 2003, s. 109). Dette skal staten gøre ved at opstille regler for individet uden at påtvinge det overbevisninger eller påvirke dets frihed.

Locke forudsætter en anden naturtilstand end Hobbes, hvor Locke anser mennesker for at være grundlæggende rationelle individer. Naturtilstanden beskrives af Locke således:

[151] Originalkilden "Two Treatise" blev publiceret første gang i 1690.

> "Men living together according to reason, without a common superior on earth, with authority to judge between them, is proberly the state of nature." (Locke, 2003, s. 108).

Modsætningen til Lockes naturtilstand eller *state of nature* er *state of war* – en tilstand der opstår, hvis et individ påføres tvang af andre. Sker dette, har individet ret til at gøre oprør mod den, der udøver denne tvang (Locke, 2003, s. 108).

Hobbes og Locke repræsenterer tydeligt to forskellige tilgange til statskonstruktionen: Absolutisme og liberalisme.[152] Det skal dog hertil bemærkes, at Hobbes i nogle sammenhænge beskrives som liberalismens grundlægger, hvilket kan forekomme paradoksalt, når han samtidigt beskrives som absolutist. Ønsket om en absolut statsmagt synes ikke umiddelbart at være foreneligt med liberalismen. Ifølge Hobbes er den absolutte tilstand af frihed den, der findes i naturtilstanden. Man er her i sin gode ret til at gøre præcis, hvad man vil. Naturtilstanden er på samme tid også en tilstand, hvor alle er i krig mod hinanden. Individer i naturtilstanden kan med andre ord ikke udnytte denne totale frihed, hvorfor de er bedre tjent med en absolut statsmagt – i sidste ende har individet mere frihed til at gøre, hvad individet ønsker, hvis det opererer inden for rammerne af en absolutistisk statskonstruktion.

Hobbes og Lockes divergerende svar på spørgsmålet om, hvordan man legitimerer magt, og hvilken magt der overhovedet er nødvendig, kan forklares med deres forskellige svar på spørgsmålet om mennesket i naturtilstanden. Hobbes mener som bekendt, at individer vil være i en konstant kamp, hvis de ikke er styret af en statsmagt. Det er således sikkerhed, der legitimerer statsmagten. Locke derimod ser mennesket som frit, og statens opgave er netop at sikre individets frihed.

Et andet perspektiv på forholdet mellem stat og individ er forsvaret af Hume. I bogen "A Treatise of Human Nature" (Hume, 1999) skriver Hume, at:

[152] Den liberalistiske ide er også nært forbundet med privathed og demokrati i den forstand, at liberalismen har det autonome individ i centrum. Dette autonome individ kan selv kritisk reflektere og foretage valg, der er nødvendige for demokratiets virke (Reiman, 1995, s.42).

> "When every individual person labours a-part, and only for himself, his force is too small to execute any considerable work; his labour being employ'd in supplying all his different necessities, he never attains a perfection in any particular art; and as his force and success are not at all times equal, the least failure in either of these particulars must be attended with inevitable ruin and misery. Society provides a remedy for these three inconveniences. By the conjunction of forces, our power is augmented: By the partition of employments, our ability encreases: And by mutual succour we are less expos'd to fortune and accidents. 'Tis by this additional force, ability, and security, that society becomes advantageous." (Hume, 1999, s. 330).

Ideen er så at sige, at individer indgår i en flok for at forøge deres kræfter. Det er ifølge Hume uhensigtsmæssigt ikke at konstruere et samfund, hvilket han begrunder på tre forskellige måder i det ovenstående. For det første kan den person, der arbejder alene, ikke udføre noget særligt arbejde. For det andet skal den person, der arbejder alene, selv udføre alle nødvendige opgaver, hvorfor personen aldrig vil opnå perfektion i forhold til nogle af disse opgaver. For det tredje kan den person, der arbejder alene, ikke vedblive med at udføre et tilfredsstillende og ensartet stykke arbejde over tid. Ifølge Hume er konstruktionen af et samfund den måde, hvorpå disse begrænsninger kan afhjælpes.

Sikkerhed er dog stadig en motivation for Hume, men således ikke med samme begrundelse som for Hobbes. Ifølge Hobbes indgår individer i en flok og organiserer en stat, fordi der er konkurrence om de knappe ressourcer, og menneskene er egoistiske. Hobbes påpeger således primært forhold omkring statens interne sikkerhed mellem individer (Hobbes, 2001, s. 57).

Hobbes absolutte perspektiv på statsmagten implicerer, at man ikke kan tale om, at individet har rettigheder – herunder retten til privathed. Afhandlingens grundantagelse er ikke forenelig med et sådant syn på forholdet mellem stat og individ. Derimod hviler afhandlingen på en ide om, at individer er frie og har retten til selv at bestemme. Der er med andre ord tale om et liberalistisk afsæt for forståelsen af den ontologiske relation mellem stat og individ. Det følger som nævnt også, at staten er mere end blot summen af individer, idet dette netop er præmissen for at kunne diskutere muligheden for, at statens

brug af overvågning i forhold til individet er problematisk og kan sætte privathed under pres.

6.1.3. FRA ET TRADIONELT TIL ET BREDT PERSPEKTIV PÅ SIKKERHED

Begrebet offentlig sikkerhed omfatter som tidligere nævnt også individuel sikkerhed, hvor referenten er individet og dermed også individets integritet. I modsætning til ideen om national sikkerhed tager individuel sikkerhed[153] udgangspunkt i en antagelse om, at det er individet, der er den primære referent for sikkerhed. Begrundelsen for ikke udelukkende at fokusere på nationens sikkerhed, der kan siges at være det stats-orienterede perspektiv på sikkerhed, men også på individets sikkerhed, er, at sikkerhed for en stat ikke nødvendigvis implicerer sikkerhed for individer i staten (Hiranandani, 2011, s. 1100-1101). Det er med andre ord ikke kun staten og staten som demokratisk institution, der skal sikres mod fare.

En del af begrundelsen for, at det er meningsfuldt ikke kun at tale om sikkerhed for staten, men også for individer, knytter sig til sondringen mellem en objektiv tilstand af absolut sikkerhed og en individuel sikkerhedsfornemmelse. Man kan forestille sig en stat, der er i en sådan objektiv tilstand af absolut sikkerhed. Det er i den forbindelse værd at overveje, om det overhovedet er muligt at tale om en objektiv tilstand af absolut sikkerhed på en meningsfuld måde. Det kan dog antages for en teoretisk diskussions skyld, at det kan lade sig gøre.

Ideen om objektiv sikkerhed implicerer netop, at man kan tale om, at en tilstand af absolut sikkerhed er opnået (Zedner, 2009, s. 15). Det er rimeligt at argumentere for, at dette er en ønskværdig tilstand, men næppe realiserbar. Hvis der er tale om en objektiv tilstand af absolut sikkerhed oplever staten ingen trusler. I denne stat kan der dog stadig være individer, der ikke oplever sig selv som værende sikre, idet disse individer eksempelvis kan være fattige, sultende eller syge. Individuel sikkerhedsfornemmelse refererer netop til den

[153] I afhandlingen er begrebet individuel sikkerhed konsekvent brugt som en oversættelse af det engelske human security.

subjektive oplevelse af at være i en tilstand af sikkerhed eller dets modsætning, usikkerhed. Sikkerhed her er: "[...] all in the mind [...]" (Zedner, 2009, s. 16), som Zedner udtrykker det. Det er muligt, at en følelse af usikkerhed er fuldstændigt ubegrundet. Det må dog antages, at denne følelse af usikkerhed i et eller andet omfang er afledt fra de omstændigheder, et individ befinder sig i (Zedner, 2009, s. 16).

At individet fornemmer i en tilstand af sikkerhed, betyder ikke nødvendigvis, at denne sikkerhed er til stede. Omvendt kan der også være tale om, at en tilstand af absolut sikkerhed eksisterer, uden at det enkelte individ har en oplevelse heraf. Dette forhold gælder i en situation, hvor individet ikke oplever sig selv om sikker, men kan siges at være i en tilstand af sikkerhed. Der kan også være tale om, at individet har en oplevelse af sikkerhed, og at der er god grund hertil, idet sikkerhed er til stede objektivt.

Individuel sikkerhed kan anses for at være et nyt perspektiv på sikkerhed eller et perspektiv, der komplementerer den mere traditionelle sikkerhedsopfattelse, nemlig national sikkerhed. I afhandlingen behandles individuel sikkerhed som et begreb, der komplementerer national sikkerhed. Disse to former for sikkerhed opfattes som størrelser, der ideelt set bør opretholdes på samme tid, hvilket Hiranandani også har påpeget, idet han skriver, at: "[...] human security and national security are not mutually exclusive; in fact they are mutually reinforcing." (Hiranandani, 2011, s. 1101). Perspektivet på sikkerhed, hvor både stat og individ er inddraget, er i Det Europæiske Råds Stockholm-program[154] ekspliciteret, idet der står, at:

> "Det Europæiske Råd finder, at fokus på borgernes interesser og behov bør prioriteres i de kommende år. Udfordringen vil bestå i at sikre respekt for de grundlæggende rettigheder og friheder og menneskets integritet, samtidig med at sikkerheden i Europa garanteres. Det er af afgørende betydning, at, på den ene side, retshåndhævelsesforanstaltninger og, på den anden side, foranstaltninger til sikring af individuelle rettigheder, retsstaten og interna-

[154] Stockholmprogrammet er en fastsættelse af EU's prioriteter i forhold til retfærdighed, sikkerhed og frihed fra 2010 til 2014.

> tionale beskyttelsesregler går hånd i hånd i samme retning og styrker hinanden gensidigt.“ (Det Europæiske Råd, 2010, s. 4).

Opfattelsen af sikkerhed har indtil midten af 1990'erne primært taget afsæt i en militaristisk, territorie-orienteret opfattelse. Denne opfattelse var på sit højeste under den kolde krig og er, hvad man i dag kan referere til som en traditionel forståelse af sikkerhed. I dag er sikkerhed dog ofte forstået både bredere og dybere (Paris, 2001, s. 97).

Den bredere forståelse af sikkerhed udpeger her ikke-militære trusler som: "[...] environmental scarcity and degradation, the spread of disease, overpopulation, mass refugee movements, nationalism, terrorism, and nuclear catastrophe." (Paris, 2001, s. 97). Den dybere forståelse udpeger det forhold, at man i højere grad også ser sikkerhed som et forhold, der angår individer og grupper af individer, og ikke kun som et statsanliggende i forhold til eksterne trusler.

Den traditionelle, nationale sikkerhedsforståelse har også ændret sig over tid, idet den primære trussel tidligere var indtrængen på et lands territorium, medens der i dag i højere grad er tale om dynamiske trusler, der ikke udelukkende er af militær karakter (Den Europæiske Union, 2003, s. 7). Sikkerhedstrusler på nationalt og unions-niveau i EU dækker nu til dags primært over farer såsom masseødelæggelsesvåben, organiseret kriminalitet, statssammenbrud, regionale konflikter og terror (Den Europæiske Union, 2003). I en EU-kontekst er sådanne trusler netop behandlet i EU's seneste sikkerhedsstrategi fra 2003, "A secure Europe in a better world" (Den Europæiske Union, 2003). De trusler, som EU omtaler i sikkerhedsstrategien, forekommer umiddelbart at høre under den traditionelle forståelse af sikkerhed, hvormed man søger at sikre nationen og i dette tilfælde også unionen. EU nævner dog selv, at disse trusler ikke kun er militære og dermed ikke kun skal behandles som sådan. I afhandlingen vil den nationale sikkerhed blive opfattet med afsæt i EU's sikkerhedsstrategi og de fem trusler, der er nævnt her. EU anerkender dog eksplicit i sin sikkerhedsstrategi, at individet også spiller en rolle i forhold til sikkerhed, idet det påpeges, at de fleste konflikter det seneste årti har været mellem stater, men dog med primært civile tab (Den Europæiske Union, 2003, s. 1, 4). Netop dette faktum kan være én af flere grunde til, at sikkerhed ikke

kan anskues snævert i forhold til en stat. Stat og individ er her anset for at hænge sammen.

Udvidelsen af perspektivet på sikkerhed til også at inkludere individer har sit udspring i United Nations Development Programmes (herefter UNDP) Human Development Report fra 1994, hvor dette nye og bredere syn på sikkerhed blev præsenteret første gang. UNDP argumenterede for, at sikkerhed var blevet opfattet alt for snævert som sikkerhed for et territorium. I deres rapport argumenterede UNDP for, at individers følelse af usikkerhed ofte skyldes bekymringer i dagligdagen og ikke så ofte katastrofale forhold i verden. Hvorvidt man kan få mad, om man har et job, og om ens nabolag er trykt at færdes i, er eksempler på nære forhold, der bekymrer individet (United Nations Development Programme, 1994, s. 22).

I UNDP's rapport er der ikke nogen præcis definition af individuel sikkerhed, men derimod en omfangsrig liste over komponenter, der indgår i dette sikkerhedsbegreb.[155] Dette inkluderer *økonomisk sikkerhed*, *fødevaresikkerhed*, *sundhedssikkerhed*, *miljøsikkerhed*, *personlig sikkerhed*, *samfundssikkerhed* og slutteligt *politisk sikkerhed*[156] (United Nations Development Programme, 1994, s. 24-25). Listen vidner om et særdeles inkluderende perspektiv på individuel sikkerhed, hvilket begrundes med, at de trusler, der er nævnt, afspejler de farer, som rent faktisk eksisterer for individet.

Det tydeliggøres i UNDP-rapporten, at individuel sikkerhed implicerer: "[...] freedom from fear and freedom from want." (United Nations Development Programme, 1994, s. 25). Med: "[...] freedom from fear [...]" menes der beskyttelse, således at individets overlevelse ikke trues. "[...] freedom from want."

[155] UNDP's tilgang til individuel sikkerhed kan karakteriseres som bred. En tilgang af denne type indeholder en liste af potentielle trusler, hvilket kan være alt fra krig til trusler mod individet såsom sygdom (Owen, 2004, s. 17). Modsætningen hertil ville være en smal tilgang til individuel sikkerhed, der i praksis kommer til udtryk ved, at fokus primært vil være på voldelige trusler (Owen, 2004, s. 17).

[156] Egen oversættelse af begreberne, der i UNDP's rapport er benævnt "Economic security", "Food security", "Health security", "Environmental security", "Personal security", "Community security", "Political security". (United Nations Development Programme, 1994, s. 24-25).

medfører eksempelvis, at individet skal kunne opretholde sin værdighed i form af frihed fra vold.

Individuel sikkerhed er i UNDP's optik endvidere kendetegnet ved fire karakteriska. For det første er opretholdelse af individuel sikkerhed universelt og relevant for alle individer, til trods for at intensiteten og typerne af sikkerhedsproblemstillinger kan variere.[157] For det andet er komponenterne i individuel sikkerhed afhængige af hinanden. Det vil sige, at hvis individuel sikkerhed er truet et sted i verden, vil det kunne påvirke andre steder. Eksempler herpå er terror eller organiseret kriminalitet såsom menneskehandel. For det tredje bør man forsøge at skabe individuel sikkerhed ved hjælp af præventiv indsats. For det fjerde er individuel sikkerhed centreret omkring individet (United Nations Development Programme, 1994, s. 22-23).

Individuel sikkerhed og den særdeles omfangsrige liste af begreber, der hører herunder, har dog også været kritiseret. Udover at være inkluderende er individuel sikkerhed også vagt formuleret, og dermed risikerer begrebet at lægge op til en totalitær forståelse, der betyder, at alt kan gøres til et spørgsmål om individuel sikkerhed. Her kan UNDP's liste over begreber tjene som eksempel. Paris (2001) påpeger også, at ikke alt er et spørgsmål om sikkerhed. Paris har således anført, at såfremt: "[...] human security means almost anything, then it effectively means nothing." (Paris, 2001, s. 93).

En bred definition af sikkerhed har den praktiske implikation, at definitionen bliver svær at operationalisere. Med et bredt sikkerhedsbegreb kan alt i princippet opfattes som trusler mod individet. Konsekvensen er, at et bredt perspektiv på sikkerhed kan ende med at devaluere sig selv (Liotta, 2002, s. 476; Owen, 2004, s. 19). Endnu en problemstilling, der rejser i sig i forbindelse med en bred definition af individuel sikkerhed, er, hvordan man kvantificerer sik-

[157] Samtidigt hermed må sikkerhed i høj grad ses i lyset af den kontekst, som man befinder sig i – det, der kan betegnes som en usikkerhed, vil med andre ord manifestere sig forskelligt i forskellige sammenhænge (Aquilina, 2010, s. 131; van Lieshout, Friedewald, Wright, & Gutwirth, 2013, s. 122; van Loenen, Groetelaers, Zevenbergen, & de Jong, 2007, s. 138). I rige lande kan man forestille sig, at sikkerhedstrusler er organiseret kriminalitet, narkokrig og terror. I fattige lande vil truslerne snarere være sult og fattigdom.

kerhed og eksempelvis sammenligner to landes sikkerhedsniveau. Jo bredere en definition er, desto mindre anvendelig bliver den i praksis. Desuden er det hensigtsmæssigt, at man har en fælles forståelse af et så væsentligt begreb som sikkerhed.

Der er dog et vægtigt argument bag ved ideen om det udvidede sikkerhedsperspektiv. Begrundelsen for at have et sikkerhedsperspektiv, der også inkluderer forhold såsom sult og sygdom, er blandt andet, at sådanne omstændigheder slår langt flere mennesker ihjel end eksempelvis terror (Zedner, 2009, s. 42, 45).

En mulig løsning på problemet om, i hvilken grad individets sikkerhed skal indregnes i et mere omfattende sikkerhedsbegreb, kan være at have en mere præcis definition af individuel sikkerhed. Owen (2004) har præsenteret en sådan ny definition på individuel sikkerhed, der er smallere end UNDP's definition uden dog at give køb på den grundlæggende opfattelse, at individets sikkerhed er nødvendig. Denne definition, der kan siges at befinde sig på midten af et kontinuum mellem en bred og en smal forståelse af sikkerhed, udpeger nærværende afhandlings forståelse af individuel sikkerhed og har følgende ordlyd:

> "Human security is the protection of the vital core of all human lives from critical and pervasive environmental, economic, food, health, personal and political threats" (Owen, 2004, s. 20).

Ovenstående definition, der tager afsæt i UNDP's definition, tager eksplicit afstand fra begreber som "human development" og "human well-being", som nogle definitioner på individuel sikkerhed har været kritiseret for også at inddrage (Owen, 2004, s. 20).

Anvendelsen af "the vital core" og "critical and pervasive [...] threats" i definitionen sikrer, at der er tale om sikkerhedsspørgsmål af en hvis alvor (Owen, 2004, s. 20). Med "the vital core" henvises ikke til den menneskelig krop, men derimod til det menneskelige liv. I definitionen anføres "all human lives", hvilket implicerer, at der er tale om såvel enkelte individer som grupper af individer (Owen, 2004, s. 20).

For ovenstående definition gør det sig endvidere gældende, at den ikke skal ses som et forsøg på at indregne samtlige potentielle trusler, da det ikke er muligt at fremstille en sådan fyldestgørende liste. Derimod skal definitionen opfattes som en specificering af seks relevante kategorier, der inkluderer forskellige mere konkrete trusler mod den menneskelige sikkerhed. Hermed sikres en konkret forståelsesramme omkring sikkerhedsbegrebet .

Ideen om individuel sikkerhed støttes også i en Europæisk kontekst. I 2004 udkom EU's sikkerhedsdoktrin, "A Human Security Doctrine for Europe"[158] , der omhandler muligheder i EU for at blive mere kompetent, hvad angår øgning af sikkerheden for individer og på det globale niveau. I rapporten gøres det klart, at opretholdelse af sikkerhed ikke kun er et spørgsmål om at sikre stater eller unionen i forhold de fem omtalte sikkerhedstrusler inden for EU. Sikkerhed er også blevet et globalt anliggende, der i sidste ende har indflydelse på individet. I rapporten gøres det klart, at der er et kausalt forhold mellem global sikkerhed og EU's sikkerhed, idet sikkerhed i EU er en forudsætning for global sikkerhed, ligesom global sikkerhed er en forudsætning for sikkerhed i EU (The European Union, 2004, s. 2-3). Problemer i Mellemøsten kan give anledning til terrorangreb udført i den vestlige verden, sprede sig og skabe usikkerhed hos såvel stater som individer. Ifølge EU's sikkerhedsdoktrin er individuel sikkerhed: "[...] individual freedom from basic insecurities." (The European Union, 2004, s. 4). Det tydeliggøres, at individet bør være det primære element i EU's sikkerhedsstrategi snarere end unionens grænser (The European Union, 2004, s. 5).

Afsættet for den europæiske sikkerhedsdoktrin var United Nations rapport fra 2003, "Human Security Now" (Commission on Human Security, 2003). Også her argumenteres der for et paradigmeskift i forhold til sikkerhed, således at man i højere grad tager udgangspunkt i ikke-fysiske forhold såsom menneskelige værdier. United Nations definition af sikkerhed har følgende ordlyd:

> "[...] to protect the vital core of all human lives in ways that enhance human freedoms and human fulfillment. Human security

[158] Den omtalte doktrin går også under navnet "The Barcelona Report".

> means protecting fundamental freedoms— freedoms that are the essence of life. It means protecting people from critical (severe) and pervasive (widespread) threats and situations. It means using processes that build on people's strengths and aspirations. It means creating political, social, environmental, economic, military and cultural systems that together give people the building blocks of survival, livelihood and dignity." (Commission on Human Security, 2003, s. 4).

Definitionen skal opfattes dynamisk, hvilket i praksis betyder, at "essence of life" vil variere fra person til person og fra samfund til samfund. Sikkerhed er med andre ord betinget af konteksten. Hvad der kan betegnes som en usikkerhed, vil så at sige manifestere sig forskelligt i forskellige sammenhænge (Aquilina, 2010, s. 131; van Lieshout, Friedewald, Wright, & Gutwirth, 2013, s. 122; van Loenen, Groetelaers, Zevenbergen, & de Jong, 2007, s. 138). I fattige lande vil en sikkerhedstrussel kunne omhandle forhold som sult og fattigdom. Dette er omvendt ikke en sikkerhedstrussel for hovedparten af borgerne i et land som Danmark. Netop fordi trusselsbilledet varierer, afholder UN sig også i denne sammenhæng fra at komme med en liste over begreber, der samlet set udgør individuel sikkerhed.

UN beskriver også forholdet mellem individuel sikkerhed og national sikkerhed, hvorved det bliver klart, hvorfor disse to komplementerer hinanden og ikke bør opfattes som konkurrerende paradigmer:

> "Human security and state security are mutually reinforcing and dependent on each other. Without human security, state security cannot be attained and vice versa. Human security requires strong and stable institutions. Whereas state security is focused, human security is broad." (Commission on Human Security, 2003, s. 4).

Den mere individorienterede tilgang til sikkerhed er dog kommet under pres i forbindelse med terror, hvilket kan opfattes som en tilbagegang for udviklingen heraf. Allerede et årti efter, at ideen om individuel sikkerhed vandt indpas, kom opfattelsen af nationen som den primære referent for sikkerhed tilbage. Hiranandani påpeger, at til trods for at der er sket en bevægelse fra et traditionelt syn på sikkerhed til en bredere, pluralistisk opfattelse, hvor mennesket er i centrum, så er denne ændring nemmere at få øje på i teori end i praksis. (Hiranandani, 2011, s. 1101).

6.2. SIKKERHEDSBEGREBET I UDVALGTE RETSKILDER

Sikkerhed er et komplekst genstandsfelt, som overraskende nok ikke er et særligt veldefineret i retskilder (Aquilina, 2010, s. 131; ARTICLE 29 Data Protection Working Party, 2014, s. 3). Ser man på retskilder, der omhandler sikkerhed i en EU-konktekst, så viser det sig, at sikkerhed primært er beskyttet af de enkelte medlemsstaters nationale lovgivning, hvilket er i modsætning til regulering af såvel privathed som databeskyttelse: Databeskyttelsesdirektivet, 45/95/EF, anerkender eksistensen af retten til beskyttelse af data. Ifølge Menneskerettighedskonventionen art. 8 er privatliv en ret. På globalt plan anerkender FN's verdenserklæring om Menneskerettigheder i art. 12 (De Forenede Nationer, 1948), at ingen må være genstand for vilkårlig indblanding i private forhold, familie, hjem eller korrespondance . FIP anerkender retten til, at individer skal have mulighed for kontrol over egne informationer.

Begreberne sikkerhed og privathed dækker over værdier, som giver individet mulighed for at være i en tilstand af henholdsvis sikkerhed eller privathed. I det nedenstående vil jeg af hensyn til læsevenligheden omtale sikkerhed og privathed som en "ret" eller en "rettighed".

Sikkerhed forstået som en ret til at begrænse menneskerettigheder (European Commission, 2014a, s. 35) vil blive behandlet i førstkommende afsnit. Endvidere vil sikkerhed blive belyst som en selvstændig ret, som kan komme til udtryk på to forskellige måder: Sikkerhed som en negativ individuel ret imod statens indblanding og sikkerhed som en positiv forpligtelse for staten overfor individet (van Kempen, 2013). En negativ ret implicerer, at staten afstår fra at blande sig i individets fundamentale rettigheder, hvormed individets frihed kan beskyttes. En positiv rettighed indebærer en ret til at modtage noget. I dette tilfælde vil der være tale om, at staten sikrer individet imod en fare.

Slutteligt skal det nævnes, at menneskerettigheder også kan opfattes som en måde, hvorpå international sikkerhed kan opretholdes. Antagelsen er, at beskyttelse af menneskerettigheder på nationalt plan vil understøtte international sikkerhed – et perspektiv som van Kempen refererer til som "human rights peace theory" (van Kempen, 2013, s. 4). Idet afhandlingen behandler sikker-

hed i lyset af en relation mellem stat og individ, er det ikke formålstjenligt at gå ind i en diskussion omkring denne position.

6.2.1. SIKKERHED SOM EN RET TIL AT BEGRÆNSE PRIVATHED

Det fremgår direkte af ordlyden af Menneskerettighedskonventionens art. 8, stk. 2, Ret til respekt for privatliv og familieliv (Folketingets EU-oplysning), at opretholdelse af sikkerhed kan betyde, at man må begrænse andre rettigheder som eksempelvis privathed:

> "Stk. 2. Ingen offentlig myndighed kan gøre indgreb i udøvelsen af denne ret, **undtagen forsåvidt det sker i overensstemmelse med loven og er nødvendigt i et demokratisk samfund af hensyn til den nationale sikkerhed, den offentlige tryghed eller landets økonomiske velfærd, for at forebygge uro eller forbrydelse, for at beskytte sundheden eller sædeligheden eller for at beskytte andres ret og frihed**." (min fremhævelse) (Folketingets EU-oplysning).

Det er netop den ovenfor med fed markerede undtagelse i art. 8, stk. 2, der giver mulighed for at begrænse privatheden. Staten må i nogle tilfælde begrænse retten til privathed, hvis det er nødvendigt (van Kempen, 2013, s. 13-14). Det forekommer rimeligt, at en efterretningstjeneste eksempelvis kan aflytte en person, der er mistænkt for at have begået en ulovlighed.

Sikkerhed anvendt som en ret til at begrænse paragraf 8, stk. 1 kan endvidere illustreres med en konkret dom fra Menneskerettighedsdomstolen: Leander vs. Sweden.

Leander v. Sweden (application no. 9248/81), 26th of March 1987

Torsten Leander, en svensk statsborger, påbegyndte den 20. august 1979 at arbejde som vikarierende museumstekniker på et søfartsmuseum i Karlskrona. Søfartsmuseet var placeret ved siden af Karlskrona Naval Base, hvilket er en militærzone.

Leander blev bedt om at forlade sit arbejde den 3. september 1979 på baggrund af en personlig sikkerhedskontrol af ham. Sikkerhedskontrollen blev udført i overensstemmelse med svensk lovgivning. På baggrund heraf fandt man, at han udgjorde en sikkerhedsrisiko. Leander fik ikke mulighed for at se de informationer, der lå til grund for, at han ikke kunne arbejde på museet.

Det var Leanders opfattelse, at den udførte kontrolprocedure var i strid med blandt andet Menneskerettighedskonventionens Artikel 8. Dette fik Leander ikke medhold i ved den Europæiske Menneskerettighedsdomstol. Domstolen lagde vægt på, at princippet om, at indblanding skal være i overensstemmelse med loven, var overholdt (se paragraf 52 i Leander versus Sweden).

Menneskerettighedsdomstolens dom implicerer, at statens indblanding i borgernes privatliv kan være nødvendig i et demokratisk samfund af hensyn til den nationale sikkerhed. Dommen implicer dog også, at denne adgang til indblanding skal ses i lyset af *margin of appreciation*, der er omtalt i afsnit 5.1.1.1., *Proportionalitetsprincippet i EU-ret.*

I sagen fandt man, at de rette midler var taget i brug for at beskytte national sikkerhed. Sagen kan således opfattes som en illustration af, at Menneskerettighedsdomstolen lægger mere vægt på statens interesser end det enkelte individs rettigheder og friheder (Aquilina, 2010, s. 135).

Om sikkerhed anvendt som en begrundelse for at begrænse andre rettigheder er det væsentligt at bemærke, at blot fordi man øger statens magt ved at begrænse menneskerettigheder som eksempelvis privathed, så medfører det ikke nødvendigvis, at sikkerheden også øges (van Kempen, 2013, s. 14). Der er med andre ord tale om en værdikonflikt, hvor der er to værdier i spil: Sikkerhed og privathed. Statens opgave er at realisere værdierne i lovgivningen.

I en EU-kontekst er det oplagte eksempel på denne problemstilling Logningsdirektivet, hvormed man tillod at begrænse privathed i et forsøg på at øge sikkerheden ved indsamling af metadata. Dog viste det sig, at Logningsdirektivet havde meget ringe betydning i forhold til at realisere sikkerheden som værdi i praksis. Som nævnt i introduktionen til afhandlingen blev direktivet da også erklæret for ugyldigt i 2014.

I forlængelse heraf kan man ligeledes argumentere for, at hvis eksempelvis risikoen for terror stiger, og dette får stater til at reagere ved at øge sikkerhedsforanstaltninger, så stiger risikoen ligeledes for, at menneskerettigheder som privathed eller frihed vil blive begrænset (van Kempen, 2013, s. 15). Et konkret eksempel herpå, som blev nævnt i afhandlingens introduktion, er Storbritanniens fravigelse fra Menneskerettighedskonventionens art. 5. Fravigelsen er konsekvensen af en anti-terror-pakke, der tilsiger, at bestemte grupper af mistænkte kan tilbageholdes på ubestemt tid uden retssag (Peissl, 2003, s. 19-20). Således bliver, hvad man ellers har anerkendt som væsentlige rettigheder for individer, pludselig en hindring i forhold til noget, der er vægtes højere nemlig sikkerhed (Zedner, 2009, s. 121).

6.2.2. Sikkerhed som en rettighed

Sikkerhed som en rettighed er en juridisk kodificering af en instrumentel værdi. Jeg vil i nedenstående omtale sikkerhed som en ret. Igen skal opmærksomheden henledes på, at jeg forstår en rettighed som afledt af en given værdi – i dette tilfælde sikkerhed.

Konkret kan sikkerhed som en rettighed komme til udtryk på to forskellige måder: Sikkerhed kan spille rollen som en negativ individuel ret imod statens

indblanding overfor individ. Sikkerhed kan også spille rollen som en positiv forpligtelse for staten overfor individer til at sikre dem.

6.2.2.1. SIKKERHED SOM EN NEGATIV INDIVIDUEL RET

Sikkerhed som en negativ individuel ret imod statens indblanding er en eksemplificering af den oprindelige ide med Menneskerettighedskonventionen og dermed af signifikant betydning for individets sikkerhed overfor staten. Baggrunden for, at Menneskerettighedskonventionen er blevet set i dette perspektiv, skal findes i historien. Menneskerettighedskonventionen blev vedtaget i 1950. Anden Verdenskrig havde for alvor demonstreret nødvendigheden af menneskerettigheder og væsentligheden i, at verdenssamfundet sammen tog et ansvar for disse. Kontrollen med Menneskerettighedskonventionen blev også gjort til et internationalt anliggende, idet det vidste sig, at staternes egen kontrol hermed var for tilfældig.

Den grundlæggende ide med denne anvendelse af menneskerettigheder er, at staten skal afholde sig fra at blande sig i individets fundamentale rettigheder, hvorved individets ret til frihed kan opretholdes (van Kempen, 2013, s. 10, 20). Der er så at sige tale om en form for personlig eller individuel sikkerhed.

Perspektivet på sikkerhed som en negativ individuel ret overfor staten implicerer også, at staten ikke anses for at være en upartisk part i et sikkerhedsproblem mellem stat og individ. Var staten en upartisk part, hvis opgave blot var at sikre individet imod udefrakommende fare og facilitere bestemte levevilkår, ville det ikke være nødvendigt også at sikre individet imod staten.

Sikkerhed forstået som individuel sikkerhed behandles også i art. 5 i Menneskerettighedskonventionen, hvor det står anført, at:

> "Stk. 1. Enhver har ret til frihed og personlig sikkerhed. Ingen må berøves friheden undtagen i følgende tilfælde og i overensstemmelse med den ved lov foreskrevne fremgangsmåde:
>
> a) lovlig forvaring af en person efter domfældelse af en kompetent domstol;

b) lovlig anholdelse eller forvaring for ikke-efterkommelse af en domstols lovlige påbud eller for at sikre opfyldelsen af en ved lov foreskrevet forpligtelse;

c) lovlig anholdelse eller forvaring af en person med det formål at stille ham for den kompetente retlige myndighed, når der er begrundet mistanke om, at han har foretaget en retstridig handling, eller rimelig grund til at anse det for nødvendigt at hindre ham i at foretage en retstridig handling eller i at flygte efter at have fuldbyrdet en sådan;

d) forvaring af en mindreårig ifølge lovlig kendelse med det formål at føre tilsyn med hans opdragelse eller for at stille ham for den kompetente myndighed;

e) lovlig forvaring af personer for at hindre spredning af smitsomme sygdomme, af personer, der er mentalt abnorme, drankere, narkotikere eller vagabonder;

f) lovlig anholdelse eller forvaring af en person for at hindre ham i uretmæssigt at trænge ind i landet eller af en person, mod hvem udvisnings- eller udleveringssag er svævende.

Stk. 2. Enhver, der anholdes, skal ufortøvet på et sprog, som han forstår, underrettes om grundene til anholdelsen og om enhver mod ham rettet anklage.

Stk. 3. Enhver, der anholdes eller tages i forvaring i henhold til bestemmelserne i denne artikels stk. 1 c), skal ufortøvet stilles for en dommer eller anden øvrighedsperson, der ved lov er bemyndiget til at udøve domsmyndighed, og skal være berettiget til rettergang inden for en rimelig frist, eller til at løslades i afventning af rettergang. Løsladelsen kan gøres betinget af sikkerhed for, at den pågældende giver møde under rettergangen.

Stk. 4. Enhver, der berøves friheden ved anholdelse eller forvaring, skal være berettiget til at tage skridt til, at der af en domstol træffes hurtig afgørelse om lovligheden af hans forvaring, og at hans løsladelse beordres, hvis forvaringen ikke er retsmæssig.

Stk. 5. Enhver, der har været genstand for anholdelse eller forvaring i modstrid med bestemmelserne i denne artikel, har ret til erstatning." (Folketingets EU-oplysning, art. 5).

Det fremgår af stk. 1, at "Enhver har ret til frihed og personlig sikkerhed." Det er interessant, at såvel frihed som personlig sikkerhed er nævnt som første punkt i artiklens stk. 1. I den efterfølgende del af artiklen demonstreres en opfattelse af frihed og sikkerhed som to sider af samme sag. En sådan forståel-

se af begreberne sikkerhed og frihed har sin oprindelse i den politiske filosofis liberale tænkning. John Locke er et eksempel herpå, idet han har påpeget, at grundlaget for at skabe en stat var beskyttelse af individets: "[...] life, liberty, and estate [...]" (Locke, 2003, s. 136). Begrebet "sikkerhed" er ikke defineret i art. 5. En fastlæggelse af begrebet skal i stedet findes i Menneskerettighedsdomstolens praksis. Det fremgår af domme fra Menneskerettighedsdomstolen, at retten til sikkerhed er: "[...] completely interwoven with the right to liberty and does not seem to have any practical relevance of its own" (van Kempen, 2013, s. 10). Menneskerettighedsdomstolen anser således retten til sikkerhed som særdeles nært forbundet med retten til frihed. Man kan argumentere for, at sikkerheds netop er mulighedsbetingelsen for frihed. Jeg vil dog ikke gå ind i en videre diskussion om relationen imellem disse to begreber.

At den personlige eller individuelle sikkerhed skal opfattes som nært forbundet med frihed, kommer til udtryk flere gange i ovenstående og det særligt i stk. 1, litra a -f. Heraf fremgår det eksempelvis, at en person må berøves frihed i tilfælde, hvor fremgangsmåden er: "[...] lovlig forvaring af en person efter domfældelse af en kompetent domstol; [...]". Bestemmelsen giver altså adgang til frihedsberøvelse af person. Dette kan betragtes som dels et indgreb i denne persons ret til frihed, dels en varetagelse af en anden persons ret til personlig sikkerhed. Dette bunder i en grundlæggende diskussion om retsstaten og statens voldsmonopol.

Den Europæiske Unions Charter om Grundlæggende Rettigheder behandler ligeledes retten til frihed og sikkerhed. Chartrets art. 6 lyder:

> "Ret til frihed og sikkerhed
>
> Enhver har ret til frihed og personlig sikkerhed." (Den Europæiske Union, 2010, art. 6).

Art. 6 fastslår, at sikkerhed anses for en rettighed. Bestemmelsen definerer dog ikke begrebet "sikkerhed". Nogle lande har af samme grund ønsket artiklen slettet, men i stedet er det blevet bestemt, at man fastholder anvendelsen af begrebet, og at dette skal forstås i overensstemmelse med Menneskerettighedskonventionens art. 5 (European Commission, 2014a, s. 39). Dette fore-

kommer umiddelbart hensigtsmæssigt, eftersom art. 6's ordlyd er identisk med art. 5, stk. 1, 1. pkt. i Menneskerettighedskonventionen.

6.2.2.2. SIKKERHED SOM EN POSITIV FORPLIGTIGELSE

Sikkerhed kan også opfattes som en positiv forpligtigelse for staten til at sørge for, at individet er i en tilstand af sikkerhed. Dette perspektiv tager ligesom det første perspektiv, der blev præsenteret, afsæt i en ide om, at autoriteter skal have muligheden for at krænke nogle menneskerettigheder for at opretholde sikkerhed. Sikkerhed som en positiv forpligtelse betyder, at individet skal sikres imod såvel myndigheds-relaterede personer som andre privatpersoner. Dette implicerer, at staten skal forhindre noget – der er tale om en præventiv indsats.

Heraf følger også, at staten er forpligtet til at gøre brug af relevant lovgivning med henblik på at kriminalisere, undersøge og straffe personer, der er i konflikt med gældende regler (van Kempen, 2013, s. 16). Menneskerettighedskonventionens rolle har med dette perspektiv således også undergået en fundamental forandring. Som nævnt var den oprindelige rolle for Menneskerettighedskonventionen at optræde som en individuel negativ ret imod staten. Menneskerettighederne kan nu anvendes til at legitimere og i nogle tilfælde kræve, at staten gør brug af sin magt - et skift der kan være problematisk (van Kempen, 2013, s. 16-18). Menneskerettighedskonventionen, og hvordan denne skal anvendes, lader ydermere til at være mindre gennemskuelig, idet flere interesser således skal tilgodeses og samme middel skal anvendes hertil (van Kempen, 2013, s. 20).

På baggrund af ovenstående forskellige perspektiver er det nu klart, at sikkerhed kan udlægges og opfattes forskelligt som menneskerettighed – udlægninger der endda i nogle tilfælde er i konflikt med hinanden. Desuden er det tydeligt, at sikkerhed ikke er særlig veldefineret i EU-lovgivning. Van Kempen påpeger, at der er behov for at udvikle en mere rigid definition heraf, ligesom han påpeger, at:

> "[...] international human rights law fails to provide a comprehensive, balanced view of what security means from a human rights

> perspective. As a result, human rights law offers less substance and direction to the security discourse than it potentially should be able to, while moreover this unnecessarily weakens the ability of human rights to protect the individual." (van Kempen, 2013, s. 23).

I ovenstående anerkendes det, at der kan være tale om en konflikt i forhold til større klarhed omkring sikkerhedsbegrebet og juridisk råderum. Det kan omvendt forekomme problematisk at udforme en juridisk tekst, hvori der kan indeholdes en definition af sikkerhed. Denne betragtning leder ydermere tilbage til nærværende kapitels første del, hvori sikkerhedsbegrebet netop blev diskuteret og problematiseret. Endvidere blev det demonstreret, at en definition af sikkerhed indeholder en række problematikker.

Konkret i forhold til den juridiske forståelse og praksis omkring brugen af sikkerhedsbegrebet er det ikke utænkeligt, at der omkring dette begreb eksisterer en veldefineret praksis, der er udledt af retspraksis og afsagte domme. Det falder dog udenfor afhandlingen at foretage sådanne vurderinger.

6.2.3. OFFENTLIG SIKKERHED I RELATION TIL *DATAVEILLANCE* I AFHANDLINGEN

Ovenstående diskussion tydeliggør, at individuel sikkerhed er et så omfattende begreb, at det ikke er muligt i afhandlingen at undersøge *dataveillance* som sikkerhedsteknologi i forhold til alle trusler, der kan henregnes under begrebet. Følgelig er to trusler udvalgt: Organiseret kriminalitet og terror. Disse er valgt, idet netop disse er nævnt som nøgletrusler i EU's seneste sikkerhedsstrategi. Desuden er det trusler, der kan have en indvirkning på såvel det enkelte individ som på staten.

Som det blev nævnt i begyndelsen af kapitlet, så vurderes det ikke her, at individuel sikkerhed har erstattet national sikkerhed. Det opfattes derimod således, at der nu er tilføjet endnu en dimension til sikkerhed, som før manglede i denne sammenhæng. Disse to dimensioner af sikkerhed, altså individuel sikkerhed og national sikkerhed, udgør tilsammen, hvad jeg her omtaler som offentlig sikkerhed.

Det kan måske virke som "en omvej" at definere sikkerhedsbegrebet i afhandlingen som offentlig sikkerhed bestående af to dele for derefter primært at

inddrage sikkerhedstrusler, der hører til under national sikkerhed defineret med afsæt i EU's seneste sikkerhedsstrategi fra 2003. Det er imidlertid nødvendigt, idet det netop er med til at illustrere, at sikkerhed for nationen og sikkerhed for individet anses for at være sammenhængende. Desuden demonstrerer perspektivet på sikkerhed i afhandlingen, at dette er et gode for såvel stat som individ.

7. *DATAVEILLANCE* AF *BIG DATA* SOM SIKKERHEDSTEKNOLOGI

7. *DATAVEILLANCE* AF *BIG DATA* SOM SIKKERHEDSTEKNOLOGI

Nærværende kapitel består af to hoveddele, *7.1., Big data* og *7.2., Big data som ressource for intelligence-led policing.*

Big data vil blive præsenteret, afgrænset og diskuteret i førstkommende afsnit. I de dertilhørende underafsnit vil jeg diskutere *big data* i lyset af nogle særligt centrale problemstillinger, der knytter sig til *big data*. Slutteligt vil jeg diskutere *big data* i lyset af visualisering, der er et anvendeligt værktøj til at hjælpe med bedre at kunne afkode og forstå disse *big data*. Visualisering vil blandt andet blive eksemplificeret ved social netværksanalyse.

I kapitlets anden del anskues *big data* i et mere anvendelsesorienteret lys, hvor mulighederne for anvendelse af *big data* til ILP gennem eksempler på sikkerhedsteknologier demonstreres og diskuteres. ILP er en ledelsesfilosofi, der i praksis udspiller sig ved, at en række forskellige metoder kan anvendes til, hvordan evalueret information[159] kan anvendes med henblik på at opretholde offentlig sikkerhed. Refleksioner omkring valget af sikkerhedsteknologier findes i indledningen af kapitlets anden del.

7.1. *BIG DATA*

Nogle finder, at *big data* og i særdeleshed mulighederne for anvendelse heraf markerer begyndelsen på en kæmpe transformation (Mayer-Schönberger & Cukier, 2013, s. 7). Andre hævder, at *big data* er omgivet af en utopisk retorik, der giver indtryk for et potentiale, der langt fra eksisterer (boyd & Crawford, 2012, s. 663; Richards & King, 2013, s. 45).

Hvad termen *big data* præcist dækker over, kan desuden være uklart, idet der findes hverken en officiel eller helt præcis definition heraf. En præcisering af *big data* kompliceres yderligere af, at dette er et vældigt "hypet" begreb – et

[159] "Intelligence" kan i sin simpleste form siges blot at være evalueret information (Perry, McInnis, Price, Smith, & Hollywood, 2013, s. 82).

såkaldt "buzz word" (Mayer-Schönberger & Cukier, 2013, s. 6-7). *Big data* ses dog ofte karakteriseret med udgangspunkt i tre "V'er": *Volume*[160], *velocity*[161] og *variety*[162]. Disse tre karakteristika blev nævnt for første gang i en artikel tilbage i 2001 af Doug Laney, research Vice President hos Gartner Research (Laney, 2001).[163]

Volume udpeger her ikke overraskende de mængder af data, der er til rådighed, når man taler *big data* – her vil man ifølge Laney opleve både mere bredde og dybde i de tilgængelige data (Laney, 2001, s. 1). Ifølge Wired.com (2013) produceres der omkring 2.5 quintillion bytes data hver eneste dag[164]. Det betyder helt konkret også, at 90 procent af alle de data, man har adgang til nu til dags, er generet indenfor de seneste to år, idet data genereres med ekstrem hastighed (Biehn, 2013). Kvantiteten af *big data* skal med andre ord ikke opfattes som en absolut størrelse. Derimod skal dette opfattes relativt til den tilgængelige mængde data, der er relevant i en given brugssammenhæng (Mayer-Schönberger & Cukier, 2013, s. 28).

Det andet karakteristikum, *Velocity,* henviser til anvendelse og analyse af data, der genereres med forskellig og hidtil ukendt hastighed (Laney, 2001). Denne analyse af data skal endda gerne foregå i realtid, hvilket i sig selv er en betydelig udfordring.

[160] Begrebet er ikke oversat, da der ikke findes en passende dansk betegnelse.

[161] Begrebet er ikke oversat, da der ikke findes en passende dansk betegnelse.

[162] Begrebet er ikke oversat, da der ikke findes en passende dansk betegnelse.

[163] I dag udgør de tre "V'er" første del af Gartner Researchs officielle definition på *big data*, som i sin heldhed er har følgende ordlyd: "[...] high-volume, -velocity and -variety information assets that demand cost-effective, innovative forms of information processing for enhanced insight and decision making." (Sicular, 2013).

[164] Tilbage i 2000 var omkring 25 procent af alle data i verden digitale, mens de øvrige 75 procent var på papir, magnetiske kassettebånd, vinylplader og lignende. Allerede i 2007 havde dette ændret sig drastisk. Her eksisterende omkring 300 exabytes (1 exabyte = 1 million gigabytes) gemte data, hvoraf kun 7 procent af disse var analoge (bøger, printede fotografier og så videre). De øvrige data var digitale. I 2013 eksisterede omkring 1200 exabytes i verden, hvoraf mindre end 2 procent var analoge (Mayer-Schönberger & Cukier, 2013, s. 8-9).

Det sidste af Gartners tre karakteristika, *Variety*, dækker over det forhold, at diversiteten i oprindelse af data og formatet heraf er exceptionelt store, når man taler om big data (Laney, 2001; Sicular, 2013). I dag er det heller ikke udelukkende mennesker, der genererer data, men i højere og højere grad også det såkaldte *Internet of Things,* hvilket kan opfattes som en materialisering af hele ideen om den allestedsnærværende teknologi – nok bedre kendt under den engelske betegnelse *ubiquitous computing*.

Ifølge Neil Richards (2013) kan vi forvente at se endnu mere teknologisk udstyr, der er forbundet til internettet. *Internet of Things* vil betyde, at:

> "[...] networked controls, sensors, and data collectors will be increasingly built into our appliances, cars, electric power grid, and homes, enabling new conveniences but subjecting more and more previously unobservable activity to electronic measurement, observation, and control." (Richards, 2013, s. 1940).

Internet of Things-objekter vil bidrage til den samlede mængde af *big data*, men i modsætning til eksempelvis data om telekommunikation, der primært er genereret af mennesker, vil der her være tale om data, der primært er genereret af anden teknologi (Hilbert, 2013, s. 3).

Gartners tre V'er er siden 2001 løbende blevet udvidet af forskellige parter, idet nogle vil hævde, at disse tre dimensioner ikke længere indfanger hele *big datas* kompleksitet, ligesom alle relevante karakteristika ikke beskrives. IBM har eksempelvis udvidet Gartners definition med et fjerde V: *Veracity*[165] (Siewert, 2013). Hermed udpeger IBM usikkerhed omkring data, hvilket konkret betyder: "[...] how much can data be trusted when key decisions need to made on such large volumes collected at high rates." (Siewert, 2013).

Ifølge Wired.com har flere store it-virksomheder også tilføjet yderligere to "V'er": *Viability*[166] *og Value*[167] (Biehn, 2013). Disse er begge kendetegnede ved at være mere "handlingsorienterede" end Gartners karakteristika, der er af

[165] Begrebet er ikke oversat, da der ikke findes en passende dansk betegnelse.

[166] Begrebet er ikke oversat, da der ikke findes en passende dansk betegnelse.

[167] Begrebet er ikke oversat, da der ikke findes en passende dansk betegnelse.

mere statisk og deskriptiv karakter. *Viability* handler om at undersøge, hvorvidt de massive mængder af flerdimensionelle data, man har til rådighed, er anvendelige og brugbare i en given kontekst eller til en given opgave (Biehn, 2013). Der eksisterer omgangsrige, endimensionelle datasæt med strukturerede data, hvilke ikke kan karakteriseres som *big data* med afsæt i denne forståelse *big data*. *Big data* er netop kendetegnet ved sin mangfoldighed og ved, at man i analysesammenhæng ofte anvender data fra egne systemer og ukendte kilder i kombination. I afhandlingen anlægges et bredere perspektiv på *big data*, hvor dette karakteristikum ikke spiller en så central rolle.

Viability efterfølges af *Value.* Er de *big data*, man har til rådighed, anvendelige, kan man nu frigøre værdien heraf ved at udvikle sofistikerede modeller og forespørgsler, der kan bidrage med ny viden og frembringe nye, interessante korrelationer om et givent genstandsfelt (Biehn, 2013).

Denne ide om at skabe værdi i kraft af ny viden er også indlejret i en anden definition på *big data* fra bogen "Big data A Revolution That Will Transform How We Live, Work and Think" (2013), hvori der står:

> "[...] big data refers to things one can do at a large scale that cannot be done at a smaller one, to extract new insights or create new forms of value, in ways that change markets, organizations, the relationsship between citizens and governments and more." (Mayer-Schönberger & Cukier, 2013, s. 6).

Det står nu klart, at der ikke findes en definition på begrebet *big data,* om hvilken der er konsensus. I nærværende afhandling vil jeg anse Mayer-Schönberger og Cukiers definition som en tilstrækkelig betingelse, der skal være opfyldt, for at data kan karakteriseres som *big data*. Denne definition er relevant i lyset af nærværende afhandling, idet den netop ekspliciterer et anvendelsesorienteret perspektiv på *big data*, hvor det i særdeleshed er de kvalitative muligheder med påvisning mønstre i data, der er det centrale. Dermed retter forståelsen af *big data* sig i afhandlingen også mere mod det, som blandt andre Hilbert har kaldt *big data analysis* (Hilbert, 2013, s. 4). For nemhedens skyld fastholdes dog begrebet *big data*.

Skabelsen af værdi, der sker på baggrund af en analyse, handler konkret om at få ny indsigt ud af data – *big data* handler helt basalt om forudsigelser (Mayer-Schönberger & Cukier, 2013, s. 11). Med *big data*-paradigmets indtog bevæger vi os fra et informationssamfund til et egentligt videnssamfund, hvor udfordringen nu primært består i at omdanne disse massive mængder digital information til reel viden, der kan begrunde intelligente beslutninger. Netop denne transformation af data til egentlig brugbar viden er kernen i *big data* (Hilbert, 2013, s. 4-5).

Før *big datas* invasion blev data da også primært indsamlet for at finde ud af noget bestemt – svaret på et eller flere konkrete spørgsmål. Nu kan man lade data tale, hvilket er et af de forhold, der er med til at gøre *big data* så værdifult (Mayer-Schönberger & Cukier, 2013, s. 14, 19). Med andre ord er det ikke nødvendigt at have en bestemt hypotese, man vil have be- eller afkræftet, før man indsamler data. *Big data* kan dermed også forstærke og underbygge beslutninger, der i dag blot beror på menneskelige vurderinger, og således: "[...] change fundamental aspects of life by giving it a quantitative dimension it never had before." (Mayer-Schönberger & Cukier, 2013, s. 12). Ideen om, at man nu blot kan "lade data tale", bygger også på et andet forhold, der er grundlæggende forandret med *big data*: Vi behøver ikke kun at indsamle en delmængde af de tilgængelige data. Vi kan indsamle "alle" data. I nogle sammenhænge har vi således bevæget os fra at indsamle små mængder data og behandle disse til at indsamle så meget som muligt: "N = all" som Mayer-Schönberger og Curkier udtrykker det (Mayer-Schönberger & Cukier, 2013, s. 26).

Implicit i *big data*-analyse, men også ved den mere grundlæggende ide om et videnssamfund, som omtales af Hilbert, er der en antagelse om, at verden vil blive et mere *transparent* sted med *big data*: Vi vil blive mere oplyste, og vi vil få mere *viden* om den verden, som vi lever i. Richards og King (2013) problematiserer imidlertid denne antagelse om en mere transparet verden og kalder den ligefrem for et paradoks: Indsamling af data og teknikker og værktøjer til behandling heraf er ikke selv del af en transparent proces i *big data*-sammenhæng (Richards & King, 2013, s. 41-43). Hvad der egentlig foregår, kan det med andre ord være vanskeligt eller måske ligefrem umuligt at få hold

på, idet: "[...] collection is invisible, and its tools and techniques are opaque, shrouded by layers og physical, legal, and technical Privacy by Design." (Richards & King, 2013, s. 42-43).

Idet resultater af *big data*-analyse anvendes som grundlag for beslutningstagning, kan der være gode grunde til at plædere for en større åbenhed herom i demokratiets og autonomiens navn. Det er problematisk at have et system, hvor: "[...] surveillance is a secret, or where decisions are made about individuals by a Kafaeque system of opaque and unreviewable decision-makers." (Richards & King, 2013, s. 43).

I forlængelse heraf skal det også bemærkes, at det kan diskuteres, om firmaer har en forpligtigelse til at gøre deres *big data* tilgængelige for offentligheden. Mener man, at det ikke er tilfældet, er konsekvensen, at disse firmaer har fuld kontrol med, hvem der kan få adgang til deres data. Det kan i sidste ende virke skævvridende i forhold til, hvem der har hvilke muligheder. boyd og Crawford har betegnet dette "*big data* rich" og "*big data* poor" (boyd & Crawford, 2012, s. 674).

7.1.1. Randomiserede stikprøver, eksklusion og korrelation

Det er almindeligt kendt blandt statistikere, at randomiseret stikprøveudtagning sikrer et mere præcist resultat end at inddrage flere observationer. Hvis man vil have svar på, hvad en given population mener om et binært spørgsmål, så er 1100 individuelle observationer nok – og i 19 ud af 20 tilfælde er fejlmargin indenfor 3 procent (Mayer-Schönberger & Cukier, 2013, s. 23). Dette forudsætter dog, at der rent faktisk er tale om en tilfældig stikprøveudtagning, hvilket kan være en udfordring i praksis og en planlægningstung affære. Erkendelsen af muligheden for stikprøveudtagning betød, at man har kunnet indsamle få data og få svar på spørgsmål relativt nemt og billigt. Men hele ideen hermed bygger også på, at man nødvendigvis ikke har kunnet behandle alle data. Denne tilgang til data er selvfølgelig kun et alternativ til det mest optimale, nemlig at behandle alle data. En fejlmargin på kun 3 procent lyder måske

umiddelbart imponerende, men denne fejlmargin kan jo omvendt være netop afgørende for, om resultatet overhovedet er brugbart i en given kontekst.[168]

boyd og Crawford (2012) har udfordret ovenstående ide om, at mange data er positivt, idet de store mængder data, vi har til rådighed i dag, ikke nødvendigvis betyder, at disse data også er repræsentative. Problemstillingen omkring repræsentative data eksisterer med andre ord stadig – denne problemstilling viser sig blot på en ny måde. Twitter repræsenterer eksempelvis ikke *alle* mennesker, sådan som det undertiden fejlagtigt fremstilles (boyd & Crawford, 2012, s. 669). At anvende data fra steder som sociale netværk kan medføre en række metodiske problemstillinger omkring datagrundlaget. Ydermere er det i forbindelse med Twitter uklart, hvor mange *tweets* der fjernes på grund af anstødeligt indhold, og hvor stor en andel af *tweets* det overhovedet er muligt at få adgang til fra Twitter. Lerman (2013) har i forlængelse af boyd og Crawfords kritik bemærket, at tilfældighed og sjusk[169] i data nærmest er blevet en dyd i kraft af *big data* (Lerman, 2013, s. 57). *Big data*-grundlaget kan med andre ord i nogle tilfælde være særdeles ustabilt, hvilket bevirker betydningsfulde metodiske problemer (boyd & Crawford, 2012, s. 669). I forbindelse hermed kan man stille spørgsmålstegn ved, om store mængder data korrigerer for problemer i forhold til randomiseret udvælgelse eller i virkeligheden blot forværrer dette problem (Mayer-Schönberger & Cukier, 2013, s. 22).

Ideen om at kunne behandle alle data og dermed spejle realiteterne i verden præcis, som de er, lyder særdeles tiltalende, såfremt det ellers er muligt. Der knytter sig dog en række problemer hertil, idet denne ide også forudsætter en verden, hvor personer bidrager til *big data*. Interessant er det også, at de problemer, der ofte diskuteres i forhold til *big data,* omhandler individers ret til frihed og privathed. Det er således problemstillinger, der implicit bygger på en

[168] Andre problemer relaterer sig også til tilfældig stikprøveudtagning i forbindelse med statistik. For eksempel betyder denne måde at indsamle data, at man ikke senere kan udtage en delmængde herfra og anvende disse, hvis man ønsker at besvare spørgsmål for en mere specifik gruppe. Det er dog ikke formålet med afhandlingen at diskutere dette i dybden. Det er derimod formålet her, at anskueliggøre muligheder frem for begrænsninger med *big data*.

[169] Egen oversættelse af "messiness" (Mayer-Schönberger & Cukier, 2013, s. 32, 42).

forståelse af, at subjekter er inkluderet i disse *big data*. Forudsætningen for den type problemer bygger også på en forestilling om *inklusion*: At vi nu om dage alle bidrager til *big data* (Lerman, 2013, s. 56). Det omvendte problem, *eksklusion,* eksisterer dog også i *big data.* Eksklusion kan potentielt set lede til marginalisering af dem, der slet ikke optræder i de *big data*, der efter sigende kan bruges til at "spejle" virkeligheden. Hele diskussionen omkring inklusion og eksklusion kan siges at pege tilbage til Foucault og normaliseringsbegrebet. Det normale og forventelige er, at man bidrager til denne digitale og dataficerede verden og dermed også er inkluderet i disse data på godt og ondt.

Termen dataficering betyder ifølge Mayer-Schönberger og Curkier (2013) at transformere et fænomen til et kvantitativt format, således at dette fænomen kan analyseres. Dette er væsensforskelligt fra digitalisering, der blot udpeger det at konvertere analoge data til et binært format, der er håndterbart for en computer (Mayer-Schönberger & Cukier, 2013, s. 78).

I forlængelse af ovenstående kan der argumenteres for, at en værdi som ulighed implicit kan fremmes som konsekvens af *big data* og give anledning til en usynlig eksklusion af nogle individer. Befinder man sig grundet geografi, fattigdom eller livsstil uden for denne dataficering af verden, vil man ikke være en del af *big data*-grundlaget. Det kan principielt skævvride resultater, som senere danner grundlag for beslutninger, eller blot give et forvrænget billede af, hvordan verden i virkeligheden ser ud. Paradoksalt nok bemærker Lerman, at man her taler om retten til ikke at blive glemt – *the right not to be forgotten,* hvormed Lerman med et ordspil henviser til den tidligere omtalte nye EU-lovpakke (Lerman, 2013, s. 58, 63). *The right to be forgotten* er som nævnt det populistiske navn på en del af en ny EU-lovpakke om databeskyttelse, der er under behandling. Det forventes, at denne lovpakke skal erstatte det nuværende Databeskyttelsesdirektiv 95/46/EF (Europa-parlamentet og rådets direktiv, 1995).

Det er nødvendigt at reflektere over retten til ikke at blive glemt, idet forholdet mellem "den rigtige verden" og den dataficerede verden bliver stadig sværere at få øje på (Lerman, 2013, s. 62). Personer, der af den ene eller anden

grund ikke bidrager med data, optræder af selv samme grund heller ikke i *big data*, og dermed vil en form for eksklusion implicit ske, når data behandles. I virkeligheden foranlediger denne situation, at man bør overveje om den modsatte problemstilling opstår, nemlig om *big data* også understøtter eksklusion (Lerman, 2013, s. 55-56).

En anden væsentlig debat indenfor *big data*-paradigmet og databehandling omhandler korrelation og kausalitet. Denne diskussion blev sparket i gang i 2008, da magasinet Wired udgav artiklen "The End of Theory: The Data Deluge Makes the Scientific Method Obsolete" (Anderson, 2008), hvori der stod:

> "Petabytes allow us to say: "Correlation is enough." We can stop looking for models. We can analyze the data without hypotheses about what it might show. We can throw the numbers into the biggest computing clusters the world has ever seen and let statistical algorithms find patterns where science cannot." (Anderson, 2008).

Citatet demonstrerer, at tilgængeligheden til *big data* også øger ønsket om at finde interessante korrelationer, hvilket er en del af kernen i *big data* (Mayer-Schönberger & Cukier, 2013, s. 55). Korrelationer er særligt interessante i forhold til *forudsigende analyser*[170], hvilket også inkluderer *predictive policing*. Her skal man dog være særdeles forsigtig med at tale om kausale forhold. Helt konkret betyder dette for *predictive policing*, at: "A statistical relationship between one factor and a greater crime risk does not necessarily mean that the factor "causes" the crime." (Perry, McInnis, Price, Smith, & Hollywood, 2013, s. 17). Dette kan eksemplificeres med politiets tilstedeværelse i et bestemt område med høj kriminalitet. Det betyder dermed ikke, at politiets tilstedeværelse er den udløsende årsag til høj kriminalitet (Perry, McInnis, Price, Smith, & Hollywood, 2013, s. 18). At beskrive og forstå er med andre ord to aktiviteter, der er tvingende forskellige (Hilbert, 2013, s. 30).

Denne iver efter at påpege korrelationer i dag er dog blevet problematiseret, idet den manglende etablering af kausalitet kan være problematisk (Bollier, 2010, s. 16). Helt grundlæggende består problemet i, at blot fordi der korrela-

[170] Egen oversættelse af "predictive analytics".

tion mellem to fænomener, betyder det ikke, at det ene fænomen også er årsag til det andet. Derfor gives der heller ikke mulighed for at forstå de mekanismer, der ligger til grund for en given korrelation. Sammenhænge, der kan observeres, kan have en eller flere andre faktorer som forklaring. Det er med andre ord muligt, at en korrelation er til stede, men at denne blot er et udtryk for en tilfældighed. Konsekvensen kan være, at tilfældigheder uretmæssigt tillægges en betydning, der ikke er grundlag for. Der er så at sige ingen sikkerhed, men kun sandsynligheder på spil, når man taler om korrelationer. Korrelationer har dog stadig værdi i kraft af, at sådanne kan anvendes til efterfølgende at undersøge, om der også er tale om kausalitet (Mayer-Schönberger & Cukier, 2013, s. 53).

Hvorvidt manglende fokus på kausalitet overhovedet er en relevant kritik af *big data*-analyse, er der uenighed om. Mayer-Schönberg og Cukier finder, at: "[...] society will need to shed some of its obsession for causality in exchange for simple correlations: not knowing why but only what." (Mayer-Schönberger & Cukier, 2013, s. 7).

Det må i forlængelse af ovenstående diskussion være rimeligt at konkludere, at såfremt man er opmærksom på ikke uretmæssigt at tilskrive en korrelation en kausal betydning, som ikke eksisterer, så er *big data*-analyse et anvendeligt værktøj i mange sammenhænge.

7.1.2. VISUALISERINGEN AF *BIG DATA*

Datavisualisering, der har rødder i datalogi, statistik og design, er et af de mest værdifulde midler til at gøre *big data* meningsfulde, forståelige og "menneskelige", ligesom:

> "Visualization has proven effective for not only presenting essential information in vast amounts of data but also driving complex analysis." (Keim, Qu, & Ma, 2013, s. 50).

Samme vurdering gør sig gældende i kriminalitetsanalyse, hvor visualisering beskrives som et uvurderligt værktøj (Chen, et al., 2005, s. 229). De store mængder data, vi har til rådighed i dag, betyder, at der også er et øget behov

for at kunne afkode disse data på en meningsfuld måde. Hertil kan visualisering anvendes (McKinsey Global Institute, 2011, s. 18).

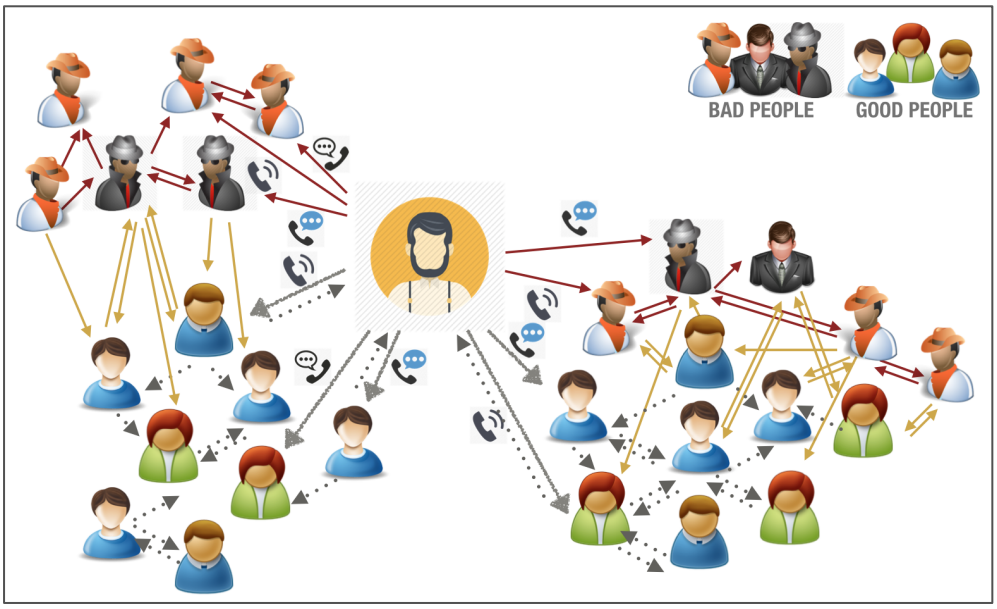
Datavisualiseringer af *big data* er typisk mere avancerede og sofistikerede end traditionelle regneark, ligesom også interaktive, brugervenlige visualiseringer med mere end to variable vinder indpas i dag (Stowers, 2013, s. 6, 10). Fremstillingen af disse visualiseringer af data er ikke udelukkende et spørgsmål om at fremvise kedelige tal og rå data på en æstetisk, interessant og smuk måde, men også et spørgsmål om at give mulighed for at repræsentere data og dermed at kunne se ukendte sammenhænge. Ydermere er visualisering et anvendeligt værktøj til at opnå en højere grad af transparens og tilgængelighed af data til et større publikum. Visualiseringer kan endvidere ses som en parallel udvikling til det tidligere omtalte Open Government Data og ideen om et mere transparent offentligt system, der sigter mod en bedre forståelse blandt borgere og en højere grad af såkaldt *citizen engagement*[171] (Stowers, 2013, s. 8-9).

Visualisering kan også med fordel finde anvendelse på kriminalitetsrelaterede data, hvor formålet kan være at understøtte politiets arbejde i forbindelse med blandt andet sociale netværksanalyser. Afdækning af sociale netværksstrukturer, personers samarbejde og det hertil knyttede "informationsflow "er af central betydning for at bekæmpe forskellige former for kriminalitet, herunder terror (Ferrara, De Meo, & Catanese, 2014; Xu & Chen, 2005).

Sociale netværksanalyser bruges til at identificere interessante personer og kortlægge sociale relationer imellem personer. Data om blandt andet venskaber, tilhørsforhold og individers pengetransaktioner kan udgøre grundlaget for en analyse. På baggrund heraf kan det bestemmes, hvem der spiller særligt centrale roller i kriminelle organisationer. Eksempelvis kræver narkosalg eller menneskehandel forskellige sociale samarbejdsrelationer. Med større kendskab til interpersonelle relationer mellem involverede personer kan man med større sikkerhed kontakte de relevante og centrale personer, hvis man vil forsøge at infiltrere et netværk den vej (Bacher, 2013, s. 23).

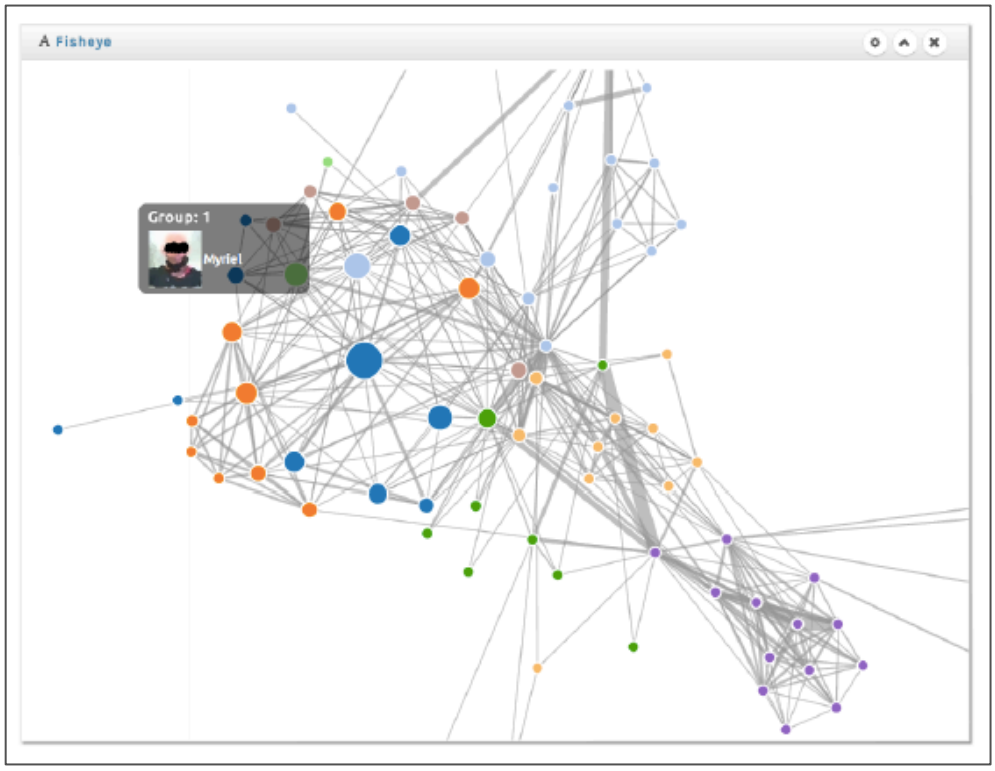
[171] Begrebet er ikke oversat, da der ikke findes en passende dansk betegnelse.

Et eksempel på en visualisering af et socialt netværk ses på billede 10, hvor visualiseringen er sket på baggrund af data om telefonopkald. Visualiseringen illustrerer de sociale cirkler, som den centrale knude (individ) beskæftiger sig med. Pilene mellem de enkelte personer repræsenterer forskellige typer af relationer: De grå pile er særligt interessante relationer, mens de gule pile er relationer mellem kriminelle og personlige kontakter til den centrale knude. Endeligt er de røde pile forbindelser mellem personer i det kriminelle netværk (Ferrara, De Meo, & Catanese, 2014).



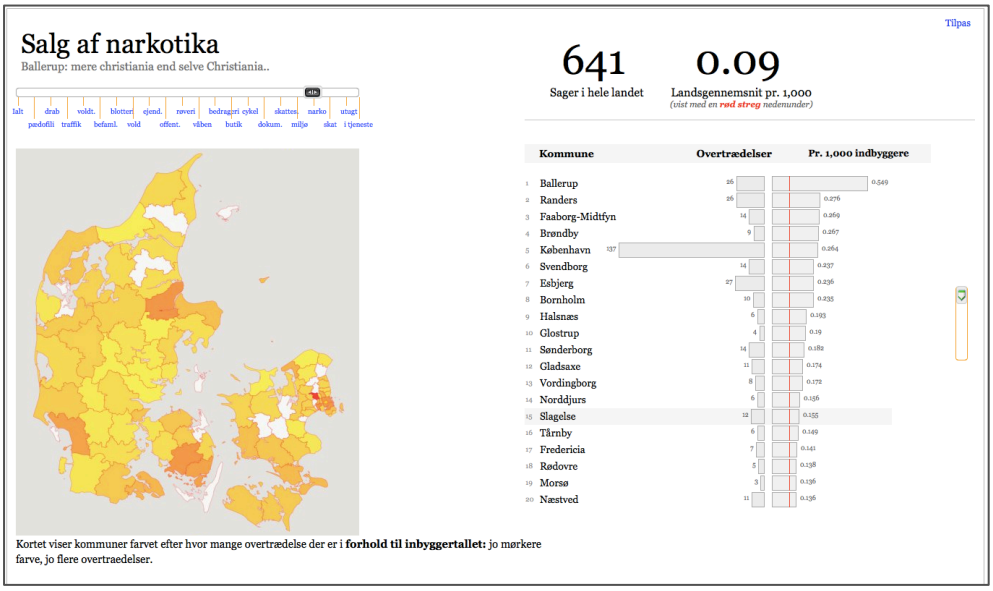
Billede 10: Visualisering af socialt netværk på baggrund af telefonopkald (Ferrara, De Meo, & Catanese, 2014)

Et andet eksempel på en visualisering af et socialt netværk findes i billede 11, der er en såkaldt *fisheye*- repræsentation, der er visualiseret på baggrund af telefonopkald mellem 75 individer. *Fisheye*- repræsentationen heraf betyder, at man kan se hele det sociale netværk på én gang, samtidigt med at en specifik del heraf kan ses i flere detaljer (Ferrara, De Meo, & Catanese, 2014).



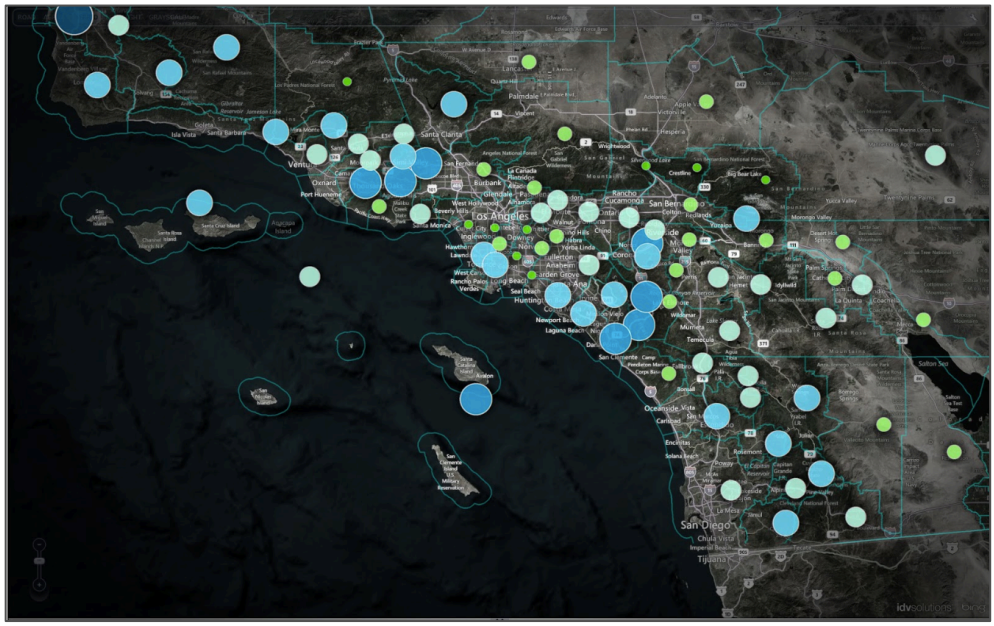
Billede 11: Fisheye-repræsentation af socialt netværk (Ferrara, De Meo, & Catanese, 2014)

Der findes også visualiseringer af kriminalitetsrelaterede data, der er udarbejdet med henblik på eksempelvis at give den enkelte borger indblik i bestemte kriminalitetsformer i bestemte geografisk afgrænsede områder. På billede 12 ses en simpel, interaktiv visualisering af anmeldte forbrydelser i Danmark i 2009 ordnet efter kommune og type af lovovertrædelse. Visualiseringen eksemplificerer, hvordan formidling og forståelse af store mængder data bliver let tilgængelig. Det er bliver hermed nemmere for den "almindelige" borger at danne sig en indtryk af fordelingen af forskellige former for kriminalitet i Danmark.



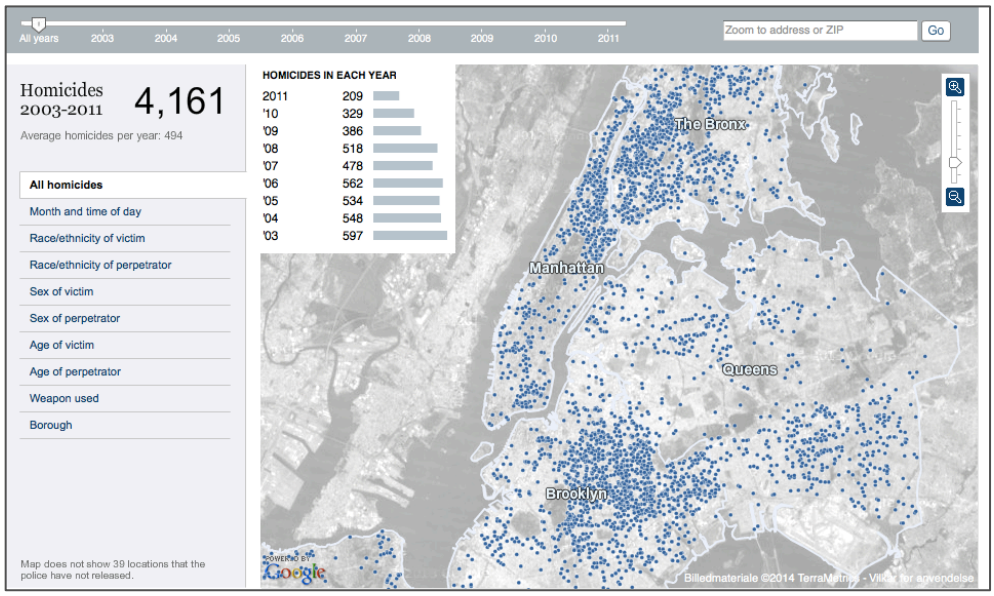
Billede 12: Visuel repræsentation af data om salg af narkotika i Danmark (http://www.smallmeans.com/datavis/kriminalitet/)

Følgende eksempel på en visualisering er udformet af et amerikansk firma (billede 13). Temaet er kriminalitet i Los Angeles, USA. De enkelte blå cirkler illustrerer et område med høj kriminalitet i forhold til det nationale gennemsnit. En sådan visualisering kan anvendes af både private og af firmaer med henblik på at bosætte sig eller drive virksomhed i de mest sikre områder af byen.



Billede 13: Visualisering af kriminalitet i Los Angeles, USA (http://4.bp.blogspot.com/-wx1V5tP3xsI/Ua4HfR2qQWI/AAAAAAAAAGQ/IsAa-PZ5WwA/s1600/CrimeIndex_LA.jpg)

Et sidste eksempel på visualisering af data stammer fra New York Times (billede 14), der har visualiseret data om mord på Manhattan og omkringliggende bydele. Der er tale om et interaktivt kort udviklet på baggrund af offentlig tilgængelige data fra New York Police Department.



Billede 14: Visualisering af mord på Manhattan og omkringliggende bydele (http://projects.nytimes.com/crime/homicides/map)

Brug af kortet giver mulighed for at få data repræsenteret på forskellig vis: Etnicitet, køn og alder på gerningsmand og offer, oversigt over dato og tidspunkt for mord eller samme data om den enkelte hændelse for blot at nævne nogle af disse visualiseringsmuligheder. Med få klik kan man finde ud af, at flest mord foretages af sorte mænd i nattetimerne. Desuden kan man med det blotte øje på ovenstående kort se, at i bydelene The Bronx og Brooklyn sker langt flest mord – godt dobbelt så mange som på selve Manhattan, hvilket også kan bekræftes af data tilgængelige ved brug af kortet.

De data, som New York Times anvender til dette interaktive kort, kan siges at skabe et problem af normativ, etisk karakter, som er svært at favne rent juridisk. Som nævnt før sigter EU's databeskyttelsesdirektiv på beskyttelse af *personhenførbare data*. [172] Dog kan der argumenteres for, at ikke-personhenførbare data også kan skabe problemstillinger, der gør etiske overvejelser relevante. Et eksempel er data, der i kraft af visualisering er blevet mere forståelige og tilgængelige og i nogle tilfælde kan bidrage til at stigmatisere en gruppe af mennesker.

Disse data er som nævnt offentligt tilgængelige og kan nu nemt tilgås af enhver med internetadgang. Den større tilgængelighed af visualiserede data kan betyde, at bestemte grupper af mennesker som for eksempel sorte mænd med bopæl i The Bronx eller Brooklyn kan føle sig stigmatiseret. På den ene side kan man argumentere for, at sådanne data ikke lyver, og at sorte mænd åbenbart er mere tilbøjelige end andre til at begå mord, hvorfor man gør klogt i at udvise særlig forsigtighed i visse tilfælde.

Man kan forestille sig, at nogle vil fremsætte et argument for, at eftersom disse data er i overensstemmelse med virkeligheden, så er der ikke noget etisk problem i at dele dem. Denne argumentation er problematisk, hvilket kan illustreres ved at drage en parallel til et dagligdags-eksempel. Informationer, der deles imellem to veninder, må også antages at være sande. Dette medfører ikke, at det vil være acceptabelt, hvis den ene veninde, med et argument om at det

[172] EU's databeskyttelsesdirektiv finder ikke anvendelse i forhold til de data, som New York Times behandler. Eksemplet er inddraget med henblik på at illustrere en teoretisk pointe.

jo er en sand information, begyndte at dele denne information med andre venner. Det er med andre ord problematisk at slutte sig til, at information i kraft af at være sand også kan eller bør deles. Og omvendt er det jo ikke *alle* sorte mænd, der begår mord, hvorfor man som sort mand, der ikke begår mord, kan føle sig uretfærdigt udpeget som tilhørende en bestemt gruppe.

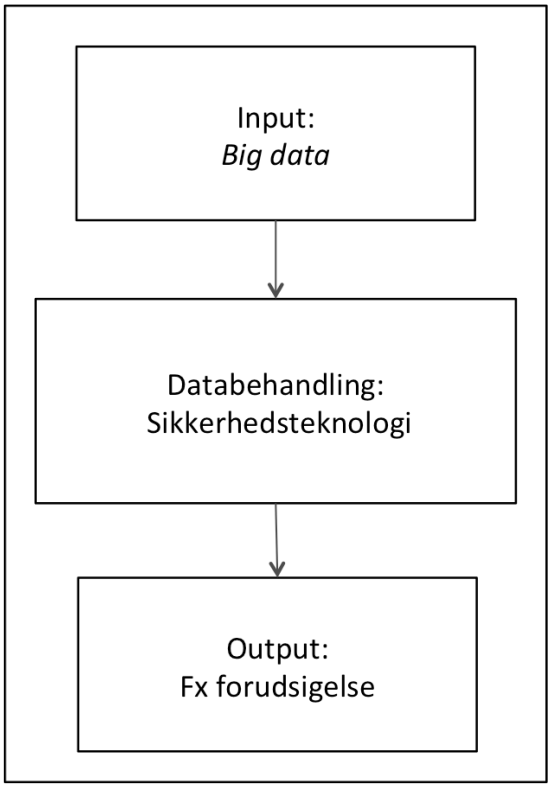
Nissenbaum har også påpeget, at der sker en forandring når data, der tidligere har været tilgængelige (digitalt eller analogt) også gøres tilgængelige online (Nissenbaum, 2004, s. 151). En betydningsfuld forskel består i mængden af personer, der kan tilgå disse – der sker bogstavelig talt en ændring fra et muligt lokalt "publikum" til et globalt (Nissenbaum, 2004, s. 151). Nissenbamm henviser også til en lovændring i USA, hvilken foreskriver, at såfremt en person der har været dømt for seksuel krænkelse af andre flytter ind i et nabolag, skal man orienteres. Der er signifikant forskel på at orientere naboer, og at gøre sådan information online for enhver. Det er ikke en uvæsentlig information for personer, der bor tæt på og eksempelvis har børn. Men spørgsmålet er, om informationen kan være relevant for en person der er bosiddende flere tusinde kilometer væk? Dette vil netop være en begrundelse for ikke at lave et offentligt tilgængeligt register, som alle kan tilgå. Men derimod blot at informere relevante personer (Nissenbaum, 2004, s. 151).[173]

Data, der her er visualiseret, har givetvis været tilgængelige længe, men den nemme (globale) tilgang hertil – og så endda i visualiseret form - gør, at man i endnu højere grad bør overveje konsekvenserne af brugen af data, og hvad visualisering betyder. Når man visualiserer *big data*, bør der ske en forudgående vurdering af måden, hvorpå data visualiseres, og dette kan have afgørende betydning for, hvordan disse data opfattes på godt og ondt.

[173] I takt med at man tillader at offentlige data gøres tilgængelige online, giver man også andre parter mulighed for at anvende disse data eksempelvis ved at sammenkøre dem med data, de enkelte firmaer selv har til rådighed (Nissenbaum, 2004, s. 151). Solove har påpeget, at muligheden for sammenkørsel af data netop er problematisk i forhold til "intet at skjule"-argumentet. Personer har måske ikke umiddelbart noget at skjule, men samtidigt ved de ikke, hvad der på baggrund af sammenkørsel kan udledes om dem (Solove, 2007, s. 766).

7.2. *BIG DATA* SOM RESSOURCE FOR *INTELLIGENCE-LED POLICING*

I nærværende afsnit vil det blive demonstreret, hvordan *big data* principielt kan bidrage til at opretholde den offentlige sikkerhed. *Big data* er her ressource for sikkerhedsteknologi, hvilket er demonstreret i nedenstående figur 4. Sikkerhedsteknologiens output kan eksempelvis være en forudsigelse.



Figur 4: Databehandling

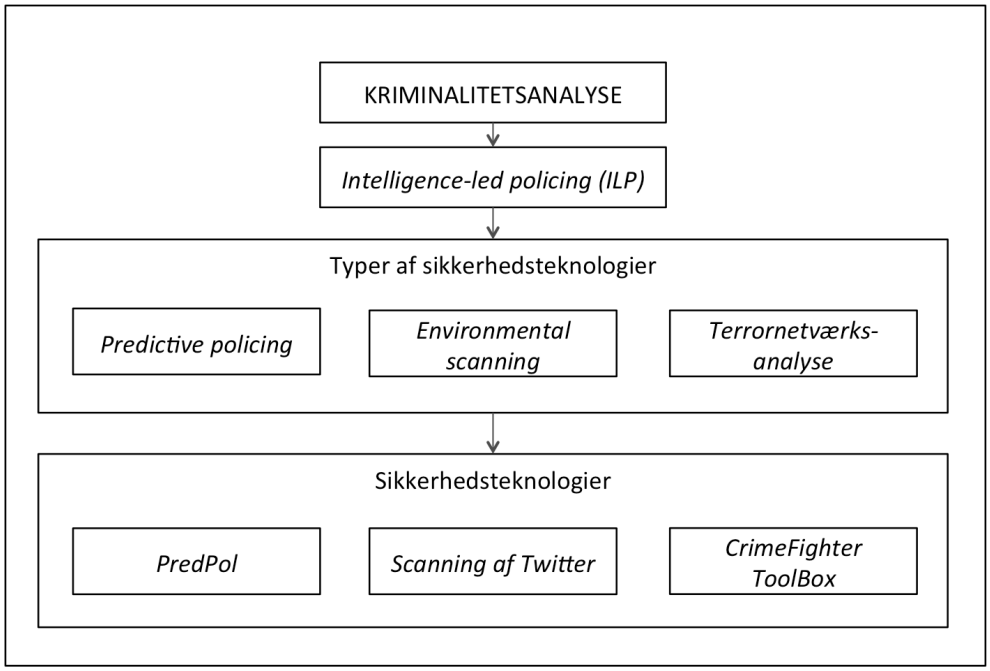
Først præsenteres ILP, der her er opfattet som en ledelsesfilosofi, der indfanger data-drevne metoder i politiarbejde. Dernæst præsenteres en række sikkerhedsteknologier, som alle hører under ILP, til opretholdelse af offentlig sikkerhed.

Konkret vil tre typer af sikkerhedsteknologier blive inddraget: *Predictive policing*, *environmental scanning* og terrornetværks-analyse. Hver af disse typer af sikkerhedsteknologier er beskrevet og diskuteret i tre separate underafsnit (7.2.3.1., *Predictive policing*, 7.2.3.2., *Environmental scanning af online-ressourcer* og 7.2.3.3., *Terrornetværksanalyse*). Hver af de tre typer af sikker-

hedsteknologier, vil blive eksemplificeret med en konkret sikkerhedsteknologi.

Predictive policing, der har et operationelt sigte, skal understøtte politiet i det daglige arbejde ved at give viden om, hvor det er mest sandsynligt, at bestemte typer af kriminelle handlinger vil forekomme. *Environmental scanning* kan have et strategisk sigte, og anvendelsen heraf beror på en ide om, at hvis man har kendskab til centrale trends i et eksternt miljø, så kan man forudsige problemstillinger, der vil opstå om eksempelvis fem, ti eller femten år. Environmental scanning kan, når det anvendes på data fra sociale medier, også have et operationelt sigte. Det er tilfældet med det eksempel, som jeg anvender i afhandlingen. Terrornetværksanalyse er ligeledes et strategisk værktøj, der kan bruges til at kortlægge terrornetværk. Systemet *CrimeFighter Toolbox* inddrages her. Antagelsen bag systemet er, at en terrornetværksanalyse er en så kompleks proces, at understøttelse i kortlægningen er nødvendig.

Nedenstående figur 5 demonstrere relationerne mellem begreber, der bliver omtalt i afhandlingen.



Figur 5: Kriminalitetsanalyse.

Hver af de omtalte sikkerhedsteknologier har formål at øge sikkerhed. Udgangspunktet for valget af de tre typer af sikkerhedsteknologier er, at de kan bidrage til at opretholde sikkerhed i forhold til en af de nøgletrusler, som er omtalt i EU's sikkerhedsstrategi (Den Europæiske Union, 2003). *Predictive policing* og *environmental scanning* kan blandt andet anvendes til at forudse organiseret kriminalitet. Terrornetværksanalyse kan, som navnet også antyder, anvendes i forhold til sikkerhedstruslen, terror.

7.2.1. SIKKERHEDSTEKNOLOGIERNES ROLLE I AFHANDLINGEN

I indeværende afsnit vil jeg begrunde, hvilken rolle sikkerhedsteknologierne har mere overordnet i afhandlingen.

Sikkerhedsteknologi kan anvendes til at opretholde sikkerhed. Det er, som det blev gjort klart allerede indledningsvist i afhandlingen, begrundelsen for, at Logningsdirektivet i sin tid blev implementeret. Det er også begrundelsen for NSA's anvendelse af XKeyscore og det britiske GCHQ's overvågning af data tappet fra fiberoptiske kabler. I nærværende kapitel belyser jeg ikke de sikkerhedsteknologier, som anvendes konkret af NSA, GCHQ eller Logningsdirektivet i EU. Derimod behandles tre sikkerhedsteknologier, som potentielt kan anvendes af en stat med henblik på at opretholde sikkerhed.

Jeg har valgt at inddrage tre sikkerhedsteknologier, som enten anvendes eller principielt *kan* anvendes af et offentligt organ til at opretholde sikkerheden. For to af sikkerhedsteknologierne, *environmental scanning af Twitter* og terrornetværksanalyse-teknologien C*rimefighter Toolbox*, gør det sig endvidere gældende, at teknologierne ikke relateres direkte til eksisterende anvendelse heraf i nuværende praksis. Formålet med at inddrage de udvalgte sikkerhedsteknologier er, at disse sikkerhedsteknologier kan udgøre *et scenarie*, som danner grundlag for at illustrere og diskutere spændingen mellem offentlig sikkerhed og informationel privathed. Sikkerhedsteknologierne udgør på den måde et mere konkret diskussionsgrundlag med henblik på at kunne illustrere teoretiske pointer. Ideen er, at sikkerhedsteknologierne kan demonstrere nogle muligheder for anvendelse i forhold til at kunne opretholde sikkerhed.

I stedet for at anvende sikkerhedsteknologierne som et scenarie kunne jeg have forsøgt at få indblik i nogle helt konkrete sikkerhedsteknologier, der anvendes i praksis. Det er dog fravalgt af flere grunde. For det første er det usandsynligt, at det overhovedet ville være muligt at få tilstrækkeligt kendskab til en sikkerhedsteknologi, der anvendes i praksis, til at denne teknologi kunne behandles her. En anden mulighed er at opnå kendskab til konkret sikkerhedsteknologi gennem sekundære kilder. Kigger man på sikkerhedsteknologierne, som anvendes af NSA, er det primære grundlag for at behandle eksempelvis XKeyscore de afsløringer, som Edward Snowden er kommet med gennem The Guardian og er publiceret i bogen "No Place to Hide" (Greenwald, 2014). Det kan vise sig at være problematisk at lade sådanne afsløringer danne grundlag for en mere omfattende beskrivelse af en sikkerhedsteknologi, af den grund at de oplysninger, der er til rådighed, ikke nødvendigvis er tilstrækkelige. Desuden er det svært at verificere oplysningerne. Der er dog tilstrækkeligt materiale til rådighed omkring sikkerhedsteknologien *PredPol* til, at jeg har valgt at inddrage denne.

Fordelen ved at inddrage sikkerhedsteknologi, som anvendes eller principielt kan anvendes med det formål at øge sikkerheden, men som samtidigt ikke er koblet op på en konkret anvendelse i praksis, er, at emnet for diskussion ikke "drukner" i omkringliggende informationer om en sådan case. Det ville være uhensigtsmæssigt, idet formålet med behandling af sikkerhedsteknologier er ikke at diskutere en sikkerhedsteknologi i en konkret praksis, men derimod at bruge denne sikkerhedsteknologi med henblik på at udpege nogle generelle forhold omkring spændingen mellem offentlig sikkerhed og privathed i sikkerhedsteknologier. I forhold til *PredPol* skønner jeg, at til trods for at denne teknologi anvendes i praksis, så er det stadig relevant at inddrage denne. Desuden anvendes der ikke direkte personhenførebare data i *PredPol*, hvilket dog giver mulighed for at diskutere en række andre pointer i forbindelse hermed – eksempelvis kategorisering af individer. Denne problemstilling er flere gange rejst i afhandlingen.

Tidligere i afhandlingen er der etableret et argument for, at værdierne informationel privathed som offentlig sikkerhed begge har betydning for både stat,

samfund og individ. Formålet med at belyse en række udvalgte sikkerhedsteknologier er at diskutere og vurdere spændingen mellem værdier og sikkerhedsteknologi. Ydermere danner sikkerhedsteknologien *PredPol* også grundlag for at kunne diskutere stigmatisering.

Det skal nævnes, at nogle af diskussionerne omkring værdier i sikkerhedsteknologierne og problematisering heraf først findes i kapitel 8., *Realisering af værdier i design.*

7.2.2. INTELLIGENCE-LED POLICING

Brugen af data i arbejde med kriminalitet er ikke en ny ide, idet man længe har kendt til såkaldte *crime maps* og herunder også *hotspot maps.* Analyse af kriminalitet i bred forstand går tilbage til starten af det nittende århundrede, hvor man for første gang i 1829 kortlagde og dermed "visualiserede" data om indbrud i Frankrig. En etnograf og en advokat stod bag dette arbejde, hvor statistisk materiale fra årene 1825-1827 blev inddraget til at udvikle kort over kriminalitet mod huse, personer samt uddannelsesniveau blandt personer bosiddende i forskellige områder af Frankrig. Resultatet af undersøgelsen blev blandt andet, at i områder med megen kriminalitet mod huse kunne der påvises mindre kriminalitet mod mennesker. Ligeledes fandt man ud af, at et højere uddannelsesniveau blandt beboere i et område betød mere kriminalitet mod huse (Weisburd & McEvan, 1997, s. 5).

Anvendelsen af mere moderne statistiske og geo-spatiale analysemetoder i politiarbejde er ikke ny, men har været kendt i flere årtier (Perry, McInnis, Price, Smith, & Hollywood, 2013, s. 2). Der er dog sket en bevægelse fra mere simple heuristiske metoder til anvendelsen af avancerede, matematiske algoritmer i forbindelse hermed.

I 1980erne og 1990erne så man de første tegn på ILP i Storbritannien. Brugen af data blev fra starten af 1990erne mere almindelig praksis i politiets arbejde, hvor anvendelse af ILP tog afsæt i et ønske om besparelser (Ratcliffe, Intelligence-led Policing, 2003, s. 2). Siden hen er de tekniske muligheder i form af it-udstyr til at indsamle, vedligeholde og analysere data vokset betragteligt, hvilket er forhold, der alle giver grobund for data-drevet politiarbejde (Perry,

McInnis, Price, Smith, & Hollywood, 2013, s. 2). Efter 11/9 2001 og det efterfølgende terrorangreb i London har det britiske politi haft en særlig stor interesse i data-drevet politiarbejde blandt andet for at bekæmpe organiseret kriminalitet og terror (Brewster, et al., 2014a, s. 8).

ILP er en strategi, der er en del af et større område, nemlig *kriminalitetsanalyse*[174]. Den grundlæggende antagelse, som ILP hviler på, er, at en proaktiv tilgang til kriminalitet er mere hensigtsmæssig og effektiv end at tilgå kriminalitet reaktivt og på *case-by-case* niveau (Rønn, 2013, s. 54). En sådan ændring i kriminalitetsbekæmpelse, hvor der ydes en indsats på forskellige niveauer, er umiddelbart tiltalende.

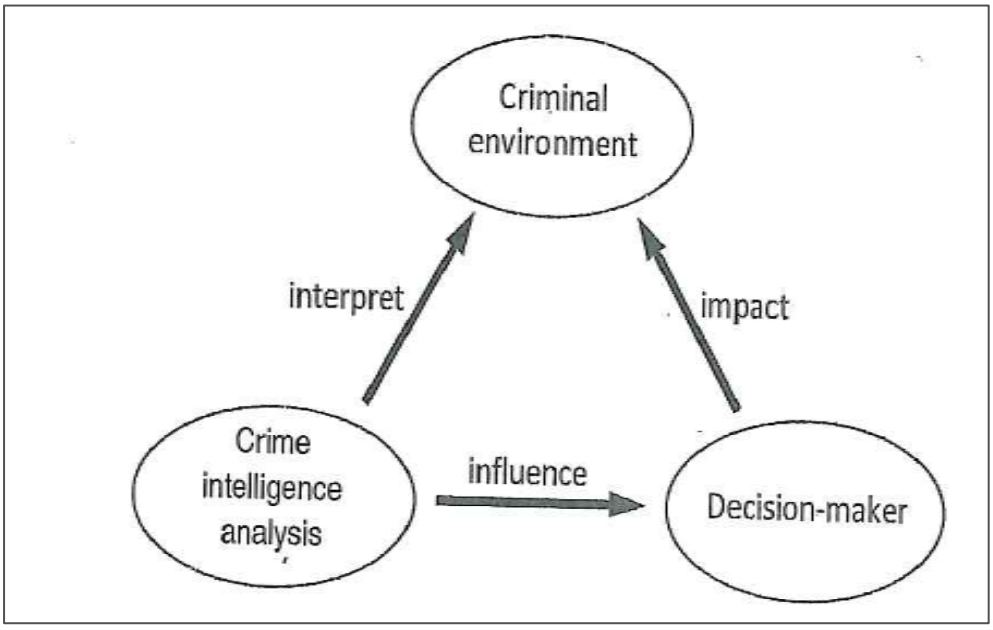
I nogle tilfælde omtales ILP som *information-led policing, prediction-led policing*, *data-driven policing, intelligence-driven policing* og *crime prediction*. Mangfoldigheden af termer, der beskriver samme eller nogenlunde ens genstandsfelter, er således stor. Jeg vil i afhandlingen anvende termen ILP, som af Ratcliffe er defineret som:

> "[...] is a business model and managerial philosophy where data analysis and crime intelligence are pivotal to an objective, decision-making framework that facilitates crime and problem reduction, disruption and prevention through both strategic management and effective enforcement stategies that target prolific and serious offenders." (Ratcliffe, 2011, s. 89).

Denne definition indfanger meningen med ILP i afhandlingen. Definitionen indrammer desuden de forskellige metoder til data-drevet politiarbejde, som virker med henblik på at opretholde offentlig sikkerhed, hvilket som nævnt vil blive eksemplificeret i senere underafsnit, hvor konkrete metoder også diskuteres.

Ratcliffe har udarbejdet modellen på billede 15, hvoraf den ideelle proces i ILP til reduktion af kriminalitet fremgår.

[174] Egen oversættelse af "crime analysis".



Billede 15: 3-i model (Ratcliffe, 2011, s. 110).

Ifølge modellen, der beskriver idealet for ILP, skal *crime intelligence analysis* bruges til at forstå (*interpret* i modellen) det kriminelle miljø. Pilen, der går fra *crime intelligence analysis* til *criminal environment,* betyder, at den aktivitet, det er at indsamle information og forstå denne, er en handling, hvor man aktivt finder den information, der er brug for (Ratcliffe, 2011, s. 110). På baggrund af den forståelse, som analytikere har opnået om et kriminelt miljø, kan analytikere nu kvalificere beslutningstagere (*decision-maker* i modellen). Ratcliffe nævner, at der kan være et problem herved, idet analytikere ikke ønsker at komme med egentlige anbefalinger til beslutningstagere. Slutteligt vil beslutningstagere øve indflydelse (*impact* i modellen) på det kriminelle miljø og tilfredsstille formålet, nemlig kriminalitetsreduktion (Ratcliffe, 2011, s. 110-111). Netop forsøget på at reducere kriminalitet (*impact* på *criminal environment*) er ifølge Ratcliffe en nødvendig betingelse for, at man kan tale om ILP. Såfremt kun interpret og influence optræder, er der ikke tale om ILP (Ratcliffe, 2011, s. 112) .

Den grundlæggende ide med ILP bygger således på en antagelse om, at viden om det kriminelle miljø er en effektiv måde at nedsætte kriminalitet på. Ydermere er ressourceallokering også en af de centrale muligheder ILP giver.

Her er antagelsen, at de største trusler skal have mest opmærksomhed. I praksis betyder det, at det nødvendigvis skal kunne bestemmes, hvad en trussel er, og det skal være muligt at sammenligne en trussel med andre trusler. Endeligt skal disse trusler kunne vægtes i forhold til hinanden (Rønn, 2013, s. 55).

Brugen af ILP medfører desuden, at beslutninger, som tidligere primært har hvilet på den menneskelige erfaring, instinkter og intuition, nu underbygges med mere eksakt data-drevet viden. Der kan endda argumenteres for, at datadrevne beslutninger vil betyde en tilsidesættelse af menneskelige vurderinger i takt med, at vi bliver bedre og bedre til at foretage sådanne forudsigende og fremtidsorienterende analyser (Mayer-Schönberger & Cukier, 2013, s. 140 - 141). Ideen med datadrevne, objektive beslutninger er umiddelbart tiltalende. Der er sig dog en række problemer ved at forlade sig på sådanne beslutninger.

At lade en algoritme træffe beslutninger involverer eksempelvis, at en reel vurdering og evaluering af baggrunden for beslutningerne synes umulig: Hvad er det egentlige beslutningsgrundlag? Et velkendt eksempel på et område, hvor det i høj grad er algoritmer, der styrer beslutninger, er køb og salg af aktier – deraf også navnene *black box trading* eller *algo trading*[175]. Som navnet *black box trading* netop indikerer, så ved man ikke rigtigt, hvad der egentlig foregår (Wikipedia, algorithmic trading). Black *box trading* er uigennemskueligt, idet beslutningsgrundlaget er ukendt. En lignende uigennemsigtig situation kan man forestille sig kan opstå ved brug af ILP.

Ovenstående stiller desuden spørgsmål ved, om: "[...] data analysis and crime intelligence are pivotal to an objective, decision-making framework [...]", som anført i definitionen af Ratcliffe ovenfor, overhovedet er muligt at opnå, eller om dette blot er et ønskværdigt mål? Her er det især brugen af begrebet "objektiv", der kan give anledning til diskussion. Denne diskussion blev også delvist adresseret i en tidligere diskussion i afhandlingen i afsnit 3.2.3.1., *Kategorisering: Objektivitet og informationel skade.*

Der kan argumenteres for, at antagelsen om, at ILP er eller i hvert fald, såfremt det er muligt, bør være objektiv, synes vanskelig at opretholde, som det også

[175] Begreberne er ikke oversat, da der ikke findes en passende danske betegnelser.

blev påpeget i tidligere afsnit. Mennesket må nødvendigvis stå bag behandling af data, da de algoritmer, ILP hviler på, er menneskeskabte. Dermed kan man sætte spørgsmålstegn ved, hvori det objektive består. Blot fordi databehandling udføres af en algoritme, betyder det ikke, at dette per se er objektivt.

Det er endvidere rimeligt at argumentere for, at resultater af analyser baseret på algoritmer leder til beslutninger, der kan bygge på flere variable, og at disse kan undergå avanceret statistisk behandling, men at det samtidigt er en fejl at sidestille det med fuldstændig objektivitet. Rønn påpeger også, at: "[...] the randomness still exists, but it is hidden behind the apprehension of acting according to reliable and objective intelligence-knowlegde." (Rønn, 2013, s. 58). Dette problematiserer ideen om en objektiv tilgang og beslutningstagning yderligere. Denne diskussion stiller også mere grundlæggende spørgsmålstegn ved, hvad der forstås ved objektivitet, og hvornår dette kan siges at være opnået. Diskussionen vil ikke blive yderligere udfoldet her. Dog er det rimeligt at påpege, at der ikke nødvendigvis er tale om objektivitet i ILP, men at der i højere grad er tale om data-drevne beslutninger.

I ovenstående er der stillet spørgsmålstegn ved, hvorvidt det er muligt at tale om objektiv beslutningstagning. En nødvendig betingelse for, at det overhovedet kan blive meningsfuldt at tale om, må være, at der på er klarhed omkring det, man objektivt vil behandle. Her består et andet grundlæggende problem i forhold til ILP, idet der kræves en præcis definition af de begreber, der skal behandles. Rønn (2013) har diskuteret denne problemstilling i forhold til organiseret kriminalitet, der netop er et område, hvor ILP kan finde anvendelse. Ydermere er organiseret kriminalitet også en af EU's nøgletrusler, hvorfor metoder som *predictive policing* og *environmental scanning* sigter mod blandt andet kriminalitet, der kan karakteriseres som sådan.

Rønn har påpeget, at indsatsen mod organiseret kriminalitet beror på *trussels-* og *skadebedømmelse*[176]. Der er dog en betydelig forvirring vedrørende disse begreber (Rønn, 2013, s. 56-57). Dette kan eksemplificeres med begrebet trusselsbedømmelse. En måde at tilgå begrebet trusselsbedømmelse er at

[176] Egen oversættelse af "assessments of threats and harms" (Rønn, 2013, s. 60).

inddele det i *intentioner*[177] og *evner*[178]. Man skal således både have tilstrækkelige intentioner om og evner til at udføre organiseret kriminalitet, for at man kan udgøre en trussel. Rønn bemærker i den forbindelse, at det er uklart, hvornår man har tilstrækkelige intentioner og evner, hvilket er problematisk (Rønn, 2013, s. 56). Det er selvklart problematisk at ville behandle, kvantificere og slutteligt anvende noget som beslutningsgrundlag, hvis det ikke er velafgrænset. Og selv hvis man kunne kvantificere organiseret kriminalitet, opstår en nyt problem, idet den grundlæggende ide med ILP er, at de største trusler skal have mest opmærksomhed: Men hvordan udpeges den største trussel? Hvad der er den største trussel, kan siges at være kontekst-afhængig, hvilket betyder, at man ikke kun udforme nogen eviggyldig måde at bestemme dette på (Rønn, 2013, s. 57).

Rønn foreslår, at ILP bliver tilgået på en måde, hun kalder en *deltagende tilgang*[179], hvormed ILP kan demokratiseres. Ideen hermed er, at prioriteringer kan foretages mere præcist, og at interessenter får et bedre indblik i de metodiske og epistemologiske problemstillinger, der eksisterer. Denne demokratisering, hvoraf der også følger større transparens for brugere af *intelligence-led polcing,* er ikke nødvendigvis løsningen på alle de ovenstående problemstillinger: Problemet omkring objektivitet i databehandlingen består for så vidt stadig. Problemstillingen bliver dog mere gennemskuelig og synlig for dem, der anvender metoden i politiarbejde. Hermed synes en del af problemet at være løst.

7.2.3. EKSEMPLIFICERING AF SIKKERHEDSTEKNOLOGIER

I nedenstående underafsnit vil forskellige sikkerhedsteknologier, der falder indenfor ILP, blive introduceret. Disse metoder demonstrerer samlet, hvordan ILP kan spille en rolle på et operationelt, taktisk og strategisk niveau. Teknologierne retter sig med andre ord med forskellige formål.

[177] Egen oversættelse af "intentions" (Rønn, 2013, s. 56).

[178] Egen oversættelse af "capabilities" (Rønn, 2013, s. 56).

[179] Egen oversættelse af "participatory approach" (Rønn, 2013).

Først vil såkaldt *predictive policing* blive introduceret, hvormed en type af en sikkerhedsteknologi, hvis formål er anvendelse i forhold til kortsigtede beslutninger, demonstreres. *Predictive policing* indeholder en lang række af forskellige typer af metoder og konkrete systemer (Perry, McInnis, Price, Smith, & Hollywood, 2013). Nogle udvalgte eksempler illustrerer, hvordan sådanne data-drevne metoder kan anvendes som et operationelt værktøj i politiets arbejde med eksempelvis indbrud og biltyveri eller som ressourceallokeringsværktøj. Konkret vil der blive fokuseret på et stykke software, som benævnes *PredPol. PredPol* hører under ILP, idet man i anvendelsen fokuserer på, hvad der kommer til at ske i fremtiden, og ikke hvad der allerede er sket (Bacher, 2013, s. 9).

Efterfølgende illustreres en anden type af ILP, nemlig *environmental scanning* af digitale ressourcer online. Formålet hermed er strategiske og langsigtede forudsigelser om fremtidige trends. I det eksemple der inddrages, kan *environmental scanning* dog også få en operationel rolle. Her eksemplificeres *environmental scannings* potentiale med *knowlegde management* og med tekstanalyse af open source data fra Twitter.

Slutteligt demonstreres det, hvordan netværksanalyse kan være et brugbart værktøj til bekæmpelse af terrorisme, idet terrornetværket kan siges netop at være kraftcenteret i terror. Analyse af terrornetværk, hvilket kan bruges i efterforskningssammenhæng, vil blive eksemplificeret med den såkaldte *CrimeFighter toolbox* software.

7.2.3.1. PREDICTIVE POLICING

Forudsigelser i forbindelse med politiets arbejde kaldes populært *predictive policing. Predictive policing* er en blandt flere termer, der udpeger samme grundlæggende ide. I en rapport fra RAND Corporation (2013) om *predictive policing* bemærkes det, at termen *forecasting (policing)* i højere grad beskriver en objektiv, videnskabelig og reproducerbar viden, mens begrebet *prediction* er en subjektiv, intuitiv og ikke-reproducerbar forudsigelse. Ligesom i RAND Corporation-rapporten anvendes i nærværende afhandling begrebet *predictive policing*, idet denne term har vundet hævd. Man kan dog med rette argu-

mentere for, at der egentlig er tale om såkaldt *forecasting policing* (Perry, McInnis, Price, Smith, & Hollywood, 2013, s. 1-2).

Predictive policing udpeger ifølge RAND Corporations rapport (2013, s. 1-2) en gruppe af metoder, der er kendetegnede ved:

> "[...] the application of analytical techniques—particularly quantitative techniques—to identify likely targets for police intervention and prevent crime or solve past crimes by making statistical predictions." (Perry, McInnis, Price, Smith, & Hollywood, 2013, s. 1-2).

Denne definition lægger netop vægt på den præventive rolle, disse teknikker kan have i forhold til sandsynlige mål, hvilket netop synes at være et centralt element.

En stigende interesse for *predictive policing* har kunnet observeres siden 2008, hvilket formentlig blandt andet kan forklares med det tiltalende navn. *Predictive policing* kan fejlagtigt konnotere en forståelse af en "krystalkugle", som kan give helt præcise anvisninger på, hvornår den næste kriminelle handling vil ske, hvor den vil ske, og hvem der vil udføre den. Af samme grund er der blevet sat spørgsmålstegn ved, om *predictive policing* vil lede til "Minority Report"-lignende tilstande (Perry, McInnis, Price, Smith, & Hollywood, 2013, s. 7). I den amerikanske film "Minority Report" fra 2002, der udspiller sig i Washington D.C. i år 2054, har specialstyrken "Precrimes" ultimativ forebyggelse som sit omdrejningspunkt. I specialstyrken arbejder tre personer, der kan forudsige fremtiden og dermed også kommende mord. Det er dermed også muligt at arrestere folk, før de udfører det mord, som "Precrime"-gruppen allerede ved, de vil udføre.

Ovenstående scenarie kan imidlertid ikke overføres til *predictive policing*, der derimod skal opfattes som et redskab, der kan understøtte og danne grundlag for mere rationel brug af politiets menneskelige ressourcer. De forudsigelser, der produceres, er sandsynligheder for, at noget vil ske, men ikke *nødvendigvis* sker. Det er med andre ord *den relative sandsynlighed* for, at en kriminel handling vil ske på et bestemt tidspunkt og i et bestemt område (Bacher, 2013, s. 7; Perry, McInnis, Price, Smith, & Hollywood, 2013, s. 7-8, 55).

Grundlæggende er *predictive policing* en proaktiv tilgang til kriminalitet, hvor formålet er beslutningstagning på baggrund af efterretninger. Dette kan eksempelvis komme til udtryk ved optimeret ressourceallokering (Bacher, 2013, s. 9-10). Analyseresultaterne kan ligeledes spille en rolle på såvel et strategisk niveau, hvor de overordnede rammer fastsættes, som på et taktisk niveau, hvor "den næste episode" udpeges. Dette kan igen have konkrete operationelle implikationer. I nærværende afsnit fokuseres på *predictive policings* taktiske og operationelle rolle.

Predictive policing kan konkret komme til at spille en rolle i forhold til organiseret kriminalitet, som er en af EU's nøgletrusler. Organiseret kriminalitet er defineret som en:

> "[...] internal threat to our security has an important external dimension: cross-border trafficking in drugs, women, illegal migrants and weapons accounts for a large part of the activities of criminal gangs. It can have links with terrorism." (Den Europæiske Union, 2003, s. 5).

Predictive policing kan blandt andet bruges til at påvise, hvor der er øget sandsynlighed for, at der vil ske indbrud i huse eller biler. Disse former for kriminalitet udføres i nogle tilfælde i organiseret form, hvor en gruppe af mennesker, der kan karakteriseres som en "indbrudsbande", står bag. Forbrydelser, der umiddelbart ser små og relativt tilforladelige ud, kan med andre ord være en lokal manifestation af organiseret kriminalitet (European Commission, 2014a, s. 15). Desuden kan amerikansk software til *predictive policing, PredPol,* også anvendes med henblik på at forudsige bandekriminalitet, hvilket også kan siges at være en form for organiseret kriminalitet.

Nedenstående model (billede 16) er en visualisering af den omfattende proces, hvor selve *predictive policing* er et centralt delelement. Af modellen fremgår det tydeligt, at *predictive policing* er et redskab, der går forud for en egentlig intervention i praksis.

Billede 16: *Prediction-led policing* business proces. (Perry, McInnis, Price, Smith, & Hollywood, 2013, s. 12)

Indsamling af data er første skridt i denne proces, idet data er hele grundlaget for *predictive policing.* Såvel kvantiteten som kvaliteten af data er central for det senere analyseresultats pålidelighed. Indsamling og opbevaring af kæmpe mængder data giver i sig selv en række udfordringer[180], idet mange af disse data vil komme fra forskellige kilder. Data skal derfor være i et anvendeligt format for overhovedet at kunne bruges (Bacher, 2013, s. 13). Analysen af disse data kan tage en række forskellige former, hvor de mest simple analysemetoder udelukkende tager historiske data i betragtning. Mere avancerede analysemetoder til *predictive policing* gør brug af mange flere forskellige variable, der kan omfatte spatiale, temporale eller interpersonelle forhold.

[180] Her vil også sikkerheden omkring opbevaring data være væsentlig. Datasikkerhed falder dog udenfor afhandlingens ramme.

Hotspot maps kan eksempelvis fremstilles på baggrund af spatiale variable[181]. På baggrund af data om spatiale forhold kan man få en større indsigt i, hvad der har betydning for områder med en høj kriminalitet, og hvilke områder der vil være populære at udføre kriminalitet i (Bacher, 2013, s. 16). Det kan eksempelvis spille en rolle, hvor mange potentielle ofre eller andre mål, der er i et område. Sådanne mål kan være steder med stor rigdom eller shopping centre. Er der gode flugtruter fra et område, herunder eksempelvis broer, tunneler eller offentlig transport, kan dette også være betydningsfuldt for, hvor attraktivt et område er for kriminelle. Ydermere indikerer fastfood-restauranter, steder med alkoholsalg og barer, at flere kriminelle bor i området (Bacher, 2013, s. 16).

En anden grund til, at *predictive policing* er muligt, er, at kriminalitet også er statisk forudsigeligt i den forstand, at kriminelle ofte opererer i deres komfort-zone. I praksis vil kriminelle udøve kriminalitet, som de tidligere har haft succes med og ofte også fysisk tæt på steder, hvor de tidligere har udført dette. Mennesket er med andre ord ikke nær så tilfældigt handlende, som man måske kan forledes til at tro (Gerber, 2014, s. 116; Perry, McInnis, Price, Smith, & Hollywood, 2013, s. 2-3). Faktisk foretager kriminelle, hvad man kan karakterisere som rationelle beslutninger om, hvor de vil foretage en kriminel handling. Sådanne rationelle beslutninger om en kriminel handling træffes med afsæt i parametre som for eksempel den geografiske lokation, offeret og risikoen for at blive opdaget. Vurderes forholdene at være gunstige, kan den kriminelle person vælge at slå til.

Som nævnt før er de analyseresultater, der produceres ved brug af *predictive policing*, blot et arbejdsredskab til at understøtte og kvalificere politiets interventioner i praksis. Analyseresultater, der er anvendelige i praksis, kan være svære at fremstille, hvorfor man tilstræber, at de, der udformer sådanne, har såvel analytisk forståelse som specifikt domænekendskab (Bacher, 2013, s. 13). Politioperationer, der hviler på dataanalyse, kan eksempelvis medføre

[181] Det er ydermere muligt at anvende temporale variable, hvor der for eksempel kan være tale om forhold som lønningsdage, vejrforhold, sportsbegivenheder og ugedag. Disse temporale forhold kan også have indflydelse på kriminalitet.

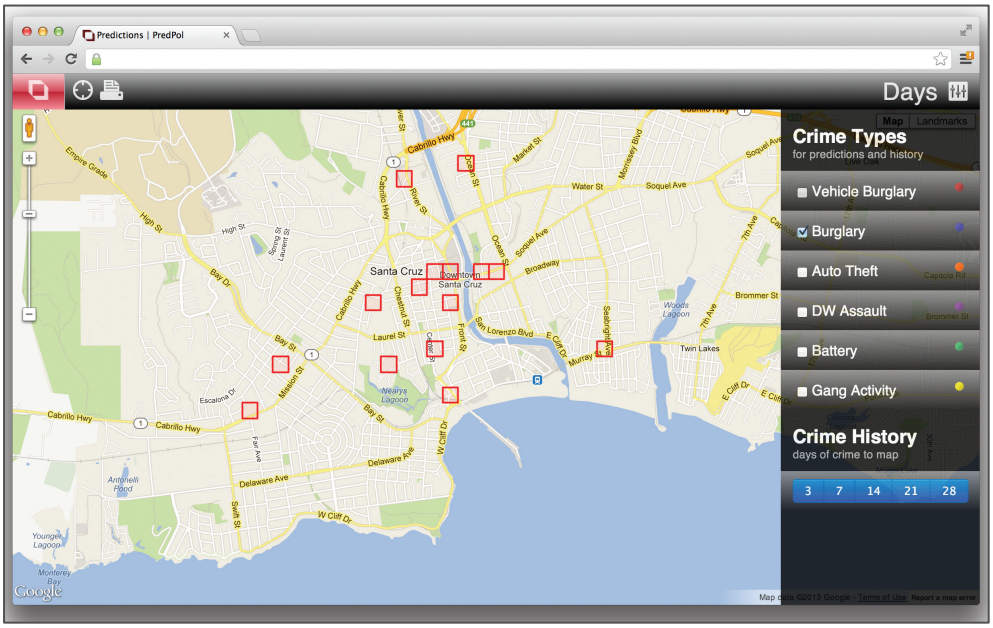
arrestationer af kriminelle eller betyde, at kriminelle stopper med at udøve kriminelle handlinger på bestemte måder eller i bestemte områder (Perry, McInnis, Price, Smith, & Hollywood, 2013, s. 13-15). Sådanne ændringer i det kriminelle mønster kan betyde, at analysens resultater forældes, idet virkeligheden forandres, hvorfor denne cyklus i politiets analysearbejde igen må påbegyndes.

Et konkret eksempel på *predictive policing* stammer fra Santa Cruz Police Department i Californien, USA, hvor man i 2011 implementerede et stykke software, *PredPol*. *PredPol* bygger på en probabilistisk analyse af historiske kriminalitets-relaterede data. Helt præcist gør *PredPol* brug af data om typen af en bestemt kriminel handling, tidspunktet her og lokationen (Bacher, 2013, s. 25-26).[182] Der indsamles ingen personlige informationer eller informationer om grupper. Formålet med *PredPol* er en kontinuerlig identifikation af geografisk afgrænsede områder, hvor der kan forventes kriminalitet i afgrænsede tidsperioder. Der er således tale om en moderne, reelt forudsigende udgave af det traditionelle *hotspot map*.

Resultatet af en *PredPol*-analyse ses på billede 17, der viser brugergrænsefladen i *PredPol*. På brugergrænsefladen ses femten[183] indtegnede felter, der alle i virkeligheden er 150 meter x 150 meter. Disse felter illustrerer, hvor det er mest sandsynligt, at de næste kriminelle handlinger vil forekomme. Desuden kan politiet få oplysninger om, hvilke typer af kriminelle handlinger, der forventes (Bacher, 2013, s. 25-26). I forbindelse med hvert vagtskifte får politimændene et kort som i billede 17, så de kan være særligt opmærksomme på de steder, hvor det er mest sandsynligt, at forskellige typer af kriminalitet vil ske.

[182] Der kan stilles spørgsmålstegn ved, om disse typer af data reelt er *big data*. Det er måske ikke den slags data, som de fleste tænker på, når de tænker på *big data*. Tager man afsæt i definitionen i afhandlingen, der stammer fra Mayer-Schoenberg og Cukiers definition, så kan sådanne data dog godt karakteriseres som *big data.* Der er tale om, at der skal en hvis volumen af data til, for at PredPol kan fungerer. Desuden kan disse data give nye indsigter.

[183] Anvendes *PredPol* i større politikredse, vil man øge antallet af høj-risiko-felter.



Billede 17: Brugergrænseflade i systemet *PredPol* (Bacher, 2013, forside)

I *predictive policing* kan analyse af spatiale variable konkret danne baggrund for beslutning om allokering af ressourcer som beskrevet i *PredPol*-eksemplet. Der er dog visse komplikationer forbundet hermed. Det geografiske afgrænsede område, som udpeges til at være et kriminelt *hotspot*, er blot en perceptuel konstruktion, idet der principielt ingen grænser er for "et område". Hvordan de data, som anvendes i en analyse, konkret bruges, vil have betydning for udfaldet af analysen. Eksempelvis vil vægtning af forskellige kriminelle aktiviteter i forhold til hinanden have en betydning for resultatet af en analyse. Det samme gør sig gældende for, hvordan man vægter et områdes karakteristika i forhold til koncentrationen af kriminelle handlinger. Ligeledes kan det være at signifikant betydning, hvor lang tid tilbage i tiden de data, som man lader være til grund for en analyse, går (Bacher, 2013, s. 18).

Ovenstående eksempler illustrerer, at resultatet af en analyse i høj grad er under menneskelig påvirkning og ikke nogen "objektiv sandhed". Opfattes analyseresultaterne som et værktøj, der kan forbedre, kvalificere og effektivisere politiets arbejde, vurderes det dog at være effektfuldt. *PredPols* konkrete virkninger er under evaluering, men præliminære resultater peger på, at *PredPol* har en positiv effekt på kriminalitet (Bacher, 2013, s. 26).

7.2.3.2. ENVIRONMENTAL SCANNING AF ONLINE-RESSOURCER

En anden type af ILP, der også kan bruges til at eksemplificere et værktøj til bekæmpelse af kriminalitet, er *environmental scanning*. *Environmental scanning,* der er en form for *knowlegde management,* kan defineres som:

> "[...] the acquisition and use of information about events, trends and relationships in an organization's external environment, the knowlegde of which would assist management in planning the organization's future in action." (Choo, 1999, s. 21).

Environmental scanning er en sikkerhedsteknologi, der kan anvendes i flere sammenhænge. Blandt disse kan nævnes private og offentlige organisationer, hvor det har været brugt til at indsamle information til ledelsen med henblik på tidlige advarsler om ændringer i det eksterne miljø (Beken, 2004, s. 488). I afhandlingen fokuseres der dog på anvendeligheden af *environmental scanning* som værktøj til bekæmpelse af kriminalitet. Nedenstående eksemplificering skal i øvrigt opfattes som netop et eksempel på, hvad *environmental scanning* kan være, idet begrebet ikke dækker over én bestemt metode hertil, men kan anvendes i praksis på forskellig vis. Dog illustrerer eksemplet en måde at scanne på, der ofte anvendes (Verfaillie, Beken, & Defruytier, 2006, s. 17, 19).[184]

Formålet med *environmental scanning* er at erkende eksterne forandringer, således at der kan responderes effektivt herpå. *Environmental scanning* anvendes primært på et strategisk niveau, hvor formålet er at forudsige centrale trends og være vidende om de ændringer, der vil ske i fremtiden – *in casu* for-

[184] Det skal nævnes, at der knytter sig en række centrale metodiske spørgsmål til anvendelsen af *environmental scanning* og de grundlæggende antagelser, som denne metodologi tager afsæt i. Der er kan eksempelvis være tale om, hvorvidt environmental scanning er en brugbar metodologi til at analysere og overvåge trends i et samfund med henblik på at understøtte beslutninger indenfor netop organiseret kriminalitet. Environmental scanning er netop en metodologi, der kan finde anvendelse i forskellige sammenhænge, men er ikke udviklet specifikt med henblik på organiseret kriminalitet. Environmental scanning er blevet kritiseret for at have intuitiv karakter, hvilket kan betyde, at særlig opmærksomhed skal gives til strukturering af scanning, således man undgår "blinde vinkler". Hvis man godtager, at environmental scanning har intuitiv karakter, så implicerer det også, at de antagelser, som indsamlingen af information beror på, synes særdeles relevante at undersøge. Scanningens validitet og det output, der kommer på baggrund heraf, må derfor evalueres i lyset heraf (Verfaillie, Beken, & Defruytier, 2006, s. 19). Disse problemstillinger falder dog uden for afhandlingens genstandsfelt at behandle i flere detaljer.

hold af betydning for kriminalitet. Beslutningstagere kan få kendskab til forandringer i det eksterne miljø, og at de har mulighed for at reagere på ændringer (Beken, 2004, s. 488).

Idet *environmental scanning* anvendes som oftest som et strategisk værktøj, hvor open source data fra officielle rapporter og nyhedsartikler kan give viden på et strategisk niveau. Disse data kan kombineres med data høstet fra sociale medier, med henblik på at kortlægge *hot spots* for kriminalitet. Således kan *environmental scanning* også får en operationel rolle, hvilket gør sig gældende for det eksempel, jeg vil anvende i afhandlingen. Der er tale om, at man kan finde svage indikatorer på kriminalitet, der kan anvendes i operationel sammenhæng (Brewster, Polovina, Rankin, & Andrews, 2014b, s. 106).

Environmental scanning, der inkluderer både at *finde information* og at s*øge efter information*, kan udformes med afsæt i en PESTEL-analyse[185], der er en kunstigt skabt, struktureret ramme, hvor et miljø inddeles i en række samfundsrelaterede domæner. Dermed er der tale om en analyse på makroniveau[186]. PESTEL er et akronym for *Political*, *Economic*, *Social*, *Technical*, *Environmental* and *Leglislative* (Beken, 2004, s. 490).

Det er muligt at udføre *environmental scanning* på forskellig vis, hvoraf fire måder nu vil blive nævnt. Først kan der sondres mellem *undirected viewing*[187] og *conditional viewing*[188] (Choo, 1999, s. 22). *Undirected viewing* betyder, at man scanner bredt og uden et specifikt sigte udover at blive informeret. *Conditional viewing* betyder omvendt, at der søges efter specifikke typer af information eller emner. Ligeledes kan man sondre mellem *informal*[189] *og formal sear-*

[185] *Environmental scanning* kan også struktureres omkring en PEST-analyse, hvilket blot indeholder de fire første domæner fra PESTEL-domænemodellen (Beken, 2004).

[186] Man kan sondre mellem mikro- og makroniveau. Mikroniveau kaldes også *competitive environment* og kan defineres som: "[...] those forces close to an organisation that affect its ability to serve its costumers and make profit." (Verfaillie, Beken, & Defruytier, 2006, s. 16).

[187] Begrebet er ikke oversat, da der ikke findes en passende dansk betegnelse.

[188] Begrebet er ikke oversat, da der ikke findes en passende dansk betegnelse.

[189] Begrebet er ikke oversat, da der ikke findes en passende dansk betegnelse.

ching[190]. *Formal searching* betyder, at der proaktivt søges efter specifik information eller information om et specifikt emne rettet mod et formål. *Informal searching* sker, når man ønsker at få en dybere forståelse for en bestemt problemstilling, men foretager sin søgning relativt ustruktureret (Choo, 1999, s. 22; Verfaillie, Beken, & Defruytier, 2006, s. 17). *Formal searching* ansees for en effektiv tilgang til *enviromental scanning* (Verfaillie, Beken, & Defruytier, 2006, s. 17).

Den information, der udgør grundlaget for en *environmental scanning,* placeres i et repositorie eller i en database, hvor informationen kan struktureres med henblik på søgning (Choo, 1999, s. 24). På baggrund af søgning kan informationen i repositoriet efterfølgende anvendes til at afdække betydningen af eksterne signaler, bestemme hvorledes vi kan anvende disse data og slutteligt, hvordan man skal reagere herpå (Choo, 1999, s. 24).

Med *environmental scanning* kan man i en kriminologi-kontekst scanne data med henblik på at finde tidlige, svage tegn på kriminalitet, før disse modnes. Sådanne scanninger kan bidrage til at nedsætte organiseret kriminalitet i form af menneskehandel, der har fået bedre levevilkår i kraft af det digitale miljø, der nu findes online (Brewster, Polovina, Rankin, & Andrews, 2014b, s. 104; EUROPOL, 2011). Anvendelsen af data i retshåndhævende myndigheders arbejde med henblik på mere kvalificerede beslutninger giver en række udfordringer på forskellig vis. Der er en række udfordringer med hensyn til hvilken form for viden, der kan indlejres i et stykke software. I den forbindelse kan man sondre mellem eksplicit viden og tavs viden (Brewster, et al., 2014a, s. 4). Eksplicit viden er kendetegnet ved at kunne udtrykkes og organiseres. Eksplicit viden er den form for viden, som man kan læse sig til i en lærebog, eller som man eksempelvis opnår ved at deltage i et træningskursus om røverihåndtering. Der kan også være tale om en protokol eller en beskrevet procedure. Denne form for viden kan lagres i tekniske systemer (Brewster, et al., 2014a, s. 4-5, 7). Tavs viden er derimod svær at lagre i et system, idet denne form for viden ikke umiddelbart kan udtrykkes verbalt (Brewster, et al.,

[190] Begrebet er ikke oversat, da der ikke findes en passende dansk betegnelse.

2014a, s. 5; Polanyi, 1983, s. 4). Tavs viden bygger ofte på erfaring og/eller intuition. I politiets arbejde kan tavs viden eksempelvis være den intuition, en politimand har, om hvorvidt en bestemt mistænkt reelt har gjort noget ulovligt og i givet fald hvorfor (Brewster, et al., 2014a, s. 5). Man kan også forestille sig en betjent, der præcist kender beskrivelsen af en procedure for, hvordan man undersøger bestemte sagstyper. At skulle udføre undersøgelsen af en bestemt sagstype kan på trods af kendskabet til beskrivelsen heraf stadig forekomme svær. Med afsæt i sondringen mellem tavs viden og eksplicit viden vil man sige, at det er den tavse viden, der vanskeligt inkorporeres og udnyttes i *environmental scanning* (Brewster, et al., 2014a, s. 5).

Idet der eksisterer tavs viden, som man ikke kan overføres til et it-system, er det væsentligt at se en sikkerhedsteknologi som *environmental scanning* som et supplement til den øvrige praksis i en organisation. Alternativet er, at man mister al den erfaring, der findes her. At lade teknologi *supplere* og *facilitere* politiets arbejde er derimod hensigtsmæssigt.

Som omtalt i foregående afsnit hører netop menneskehandel ifølge EU's sikkerhedsstrategi også under organiseret kriminalitet[191]. Menneskehandel anses i EU for en alvorlig forbrydelse, der foregår på globalt plan (Europa-Parlementets og rådets direktiv, 2011) og er her defineret som:

> "Rekruttering, transport, overførelse, ydelse af husly til eller modtagelse af en person, herunder udveksling eller overdragelse af kontrol over de pågældende, ved trusler eller ved brug af magt eller andre former for tvang, ved bortførelse, ved bedrag, ved svig, ved misbrug af magt eller udnyttelse af en sårbar position eller ved, at der ydes eller modtages betaling eller fordele for at opnå samtykke fra en person, der har kontrol over en anden person, med henblik på udnyttelse." (Europa-Parlementets og rådets direktiv, 2011, s. 6).

[191] Dette fremgår endvidere også af EU Direktiv "2011/36/EU om forebyggelse og bekæmpelse af menneskehandel og beskyttelse af ofrene herfor, og om erstatning af Rådets rammeafgørelse 2002/629/RIA." hvor der står, at: "Menneskehandel er en alvorlig forbrydelse, der ofte begås inden for rammerne af organiseret kriminalitet; det udgør en grov overtrædelse af de grundlæggende rettigheder og er udtrykkeligt forbudt i Den Europæiske Unions charter om grundlæggende rettigheder." (EU, 2011, side 1, stk. 1)

Indikatorer på menneskehandel er ofte ikke nemt tilgængelige, ligesom menneskehandlere er særdeles omstillingsparate i forhold til markedets efterspørgsel. De konkrete måder, hvorpå menneskehandel foregår, er ofte forskellige, og ruterne, der anvendes for at komme til Europa, er ikke veldefinerede (EUROPOL, 2011, s. 25). Det har dog vist sig, at blandt andet i Storbritannien bruges neglebarer i nogle tilfælde som et skalkeskjul for menneskehandelsaktiviteter, hvidvaskning af penge og cannabis-produktion. Neglebarerne som skalkeskjul vil være afsæt for en konkret eksemplificering[192] af en måde, hvorpå *environmental scanning* kan udføres (Brewster, Polovina, Rankin, & Andrews, 2014b, s. 106)

Konkret kan *environmental scanning* af open-source data anvendes som et redskab til tidligt at blive opmærksom på svage signaler på menneskehandel. Sådanne open source data kan tappes fra det sociale medie Twitter, der dermed udgør en potentielt værdifuld kilde af information. Anvendelsen af data fra Twitter gør det muligt at få indsigt i et socialt netværk som følge af den store mængde data, der nu er til rådighed online (Brewster, Polovina, Rankin, & Andrews, 2014b, s. 111).

Open source data fra Twitter falder under betegnelsen *big data*, hvis man tager afsæt Mayer-Schönberger og Cukiers tidligere omtalte definition[193]. I definitionen er der eksplicit lagt vægt på, at big data beskriver handlinger, man kan gøre med data, hvis man har disse i stort antal, og som ikke ville have været muligt ellers. Dette er tilfældet her. Desuden skal disse data kunne give nye indsigter, der kan give nye muligheder for en eller flere aktører. Dette krav er ligeledes tilfredsstillet.

[192] Eksemplet stammer fra artiklen "Knowlegde Management and Human Trafficking: Using Conceptual Knowlegde Representation, Text Analytics and Open-Source Data to Combat Organized Crime" af (Brewster, Polovina, Rankin, & Andrews, 2014b). Kun dele af Brewsters et als eksempel er her præsenteret med henblik på at give en overordnet forståelse af en metodisk tilgang til data-drevet politiarbejde.

[193] Definition: "[...] *big data* refers to things one can do at a large scale that cannot be done at a smaller one, to extract new insights or create new forms of value, in ways that change markets, organizazations, the relationsship between citizens and governments and more." (Mayer-Schönberger & Cukier, 2013, s. 6).

I analyseret form menes sådanne Twitter-data at kunne få en betydningsfuld rolle ved at kvalificere politiets arbejde yderligere med henblik på afsløring af menneskehandel (Brewster, Polovina, Rankin, & Andrews, 2014b, s. 104). *Environmental scanning* kan tage udgangspunkt i tekstanalyse, der kan defineres som: "[...] the discovery of knowledge that can be found in text archives." (Hu & Liu, 2012, s. 387). Tekstanalyse har rod i semantiske og lingvistiske discipliner. Hvordan Twitter mere konkret kan scannes beskrives i nedenstående.

Det er muligt at søge efter svage signaler i Twitter-data på baggrund af en prædefineret taksonomi, der indeholder relevante begreber om den kriminalitetsform, der skal undersøges (Brewster, Polovina, Rankin, & Andrews, 2014b, s. 112). Taksonomien er udviklet på baggrund af eksisterende viden, der blandt andet er kendskab til indikatorer på neglebarer med ulovlig aktivitet. I eksemplet er inkluderet forskellige begreber, der alle relaterer sig til unge kvinder. Taksonomien er bygget op om en boolsk syntaks, hvormed formålet er at kategorisere *tweets*, der indeholder indikationer på "ungdommelighed"[194]. I taksonomien indgår tillige ord, der refererer til børn eller kvinder[195]. Indeholder et *tweet* med tegn på ungdommelighed tillige referencer til børn eller kvinder, kan indholdet pege på mindreårige arbejdere (s. 112).

[194] Begreberne "young", "youthful", "under-age", "under age", "under 16" eller "under 18" er anvendt i eksemplet på billede 18.

[195] Begreberne "girl", "girls", "child", "children", "women", "woman", "ladies", "Ladies", "Lady", "lady" eller "she" er anvendt i eksemplet på billede 18.

Billede 18: Prædefineret taksonomi til søgning af indikatorer på menneskehandel (Brewster, Polovina, Rankin, & Andrews, 2014b, s. 112)

På samme måde som i ovenstående eksempel kan der søges efter indikatorer på bestemte lokationer og derudover også efter begreber, der indikerer "rejse til" og "ankomme fra" bestemte steder. Der kan være tale om forskellige lande eller byer, hvor man ved, at det er særligt interessant at "spotte" menneskehandel. Desuden kan der søges efter konceptet *neglebar*. Der vil ligeledes være mulighed for at anvende en dynamisk taksonomi, hvilket gør sig gældende i det tidligere omtalte Twitter-eksempel, der er udarbejdet af forskere fra University of Virginia. Det betyder i mere praktiske vendinger, at taksonomien selv "kan lære", hvilke begreber der er relevante at inddrage i taksonomien (Gerber, 2014).

Reglerne i taksonomierne i eksemplet ovenfor kan nu appliceres i et digitalt miljø, hvilket er eksemplificeret i nedenstående billede 19.

```
<?xml version="1.0" encoding="UTF-8"?>
<article>
<query>"Nail Salon" "nail bar"</query>
<authortimezone>London</authortimezone>
<doclang>en</doclang>
<body>The girls working at that new nail-bar in Leeds sure look young. I must ask them what their
secrets are for young looking skin!</body>
<LOCATION>Leeds</LOCATION>
<Categories>top\NailBar</Categories>
</article>

<?xml version="1.0" encoding="UTF-8"?>
<article>
<query>"Nail Salon" "nail bar"</query>
<authortimezone>London</authortimezone>
<doclang>en</doclang>
<body>Must have walked past 2 or 3 nail bars on the way to Elland Road this afternoon, they are
springing up all over the place!</body>
<LOCATION>Elland Road;Leeds</LOCATION>
<Categories>top\NailBar</Categories>
</article>
```

Billede 19: Eksemplificering af *environmental scanning* (Brewster, Polovina, Rankin, & Andrews, 2014b, s. 114)

I eksemplet på billede 19 skal de to body-tags eksemplificere to *tweets*, hvorfra personhenførbare informationer er fjernet. Der kan nu søges i *tweets* på baggrund af prædefinerede taksonomier. Er de definerede begreber til stede, og opfylder disse i øvrigt kravene i taksonomien, så vil der være tale om en svag indikator for kriminalitet, hvilket efterfølgende kan undersøges nærmere.

Brewster et al konkluderer, at: "[...] it is clear that a developed version of such concepts can have a real potential in the identification og tangible crime indicators in open-source data" (Brewster, Polovina, Rankin, & Andrews, 2014b, s. 114). Selvom ovenstående billede 19 er et forenklet eksempel, så giver det et indblik i, hvordan *tweets* kan få en rolle i politiets arbejde, og hvorledes dette kan lade sig gøre mere praktisk. Resultater af en analyse som ovenstående kan udover at finde anvendelse på det operationelle niveau også spille en rolle på et strategisk niveau. På baggrund af analyse vil det være muligt at kortlægge aktivitetsmønstre og mere generelle trends (Brewster, Polovina, Rankin, & Andrews, 2014b, s. 114).

For det omtalte eksempel, der omhandlede Twitter-data, gør det sig gældende, at de data, der anvendes, ikke indeholder direkte personhenførebare informationer. Det skal dog nævnes, at såfremt disse data indirekte kan henføres til én bestemt person, så er der tale om et datasubjekt, som dette er defineret i EU's Databeskyttelsesdirektiv, hvorfor sådanne data i så fald er underlagt samme juridiske ramme som data, der er direkte personhenførbare.

Det forhold, at man ikke må anvende direkte eller indirekte personhenførbare data, anses som en foranstaltning, der fremmer værdien privathed. Dog kan der omvendt argumenteres for, at brugen af data fra sociale medier som Twitter stadig kan medføre, at nogle føler, at deres privathed bliver kompromitteret i en eller anden grad. Når data gøres tilgængelige på Twitter i form af *tweet*s, må det være rimeligt at antage, at formålet ikke er at informere retshåndhævende instanser og producere data, som de kan gøres til grundlag for deres analyser i en kriminologisk forankret kontekst. Igen kan denne problemstilling med fordel rammesættes i forhold til privathed som et kontekstrelativt begreb. Rent juridisk kan *environmental scanning* være uproblematisk, men set i lyset af en normativ, etisk ramme kan dette dog give anledning til visse problemstillinger.

Data flytter sig i ovenstående eksempel med andre ord fra en kontekst til en anden, når data fra et social medie pludselig bliver politiets datagrundlag for analyse. Det kan i nogle tilfælde virke problematisk, og diskussionen her er af etisk karakter. Paradokset i ovennævnte eksempler er, at data fra sociale medier er offentlig tilgængelige. Det betyder dog omvendt ikke, at personer, der selv gør disse tilgængelige på Twitter, vil finde, at en sådan brug også nødvendigvis er acceptabel.

Perspektiver på privathed, der netop centrerer sig om den kontekstforankrede information, er som nævnt blandt andet forsvaret af Nissenbaum (Nissenbaum, 2010) og Moor (Moor J. H., 1997) – benævnt som henholdsvis *spheres of life* og *zones of privacy*. I lyset af nutidens teknologiske muligheder, som det er præsenteret ovenfor, er et perspektiv af den type for alvor med til at indfange et relevant aspekt af privathedsdiskussionen nu til dags. Denne diskussion er belyst og udfoldet i detaljer i kapitlet om privathed.

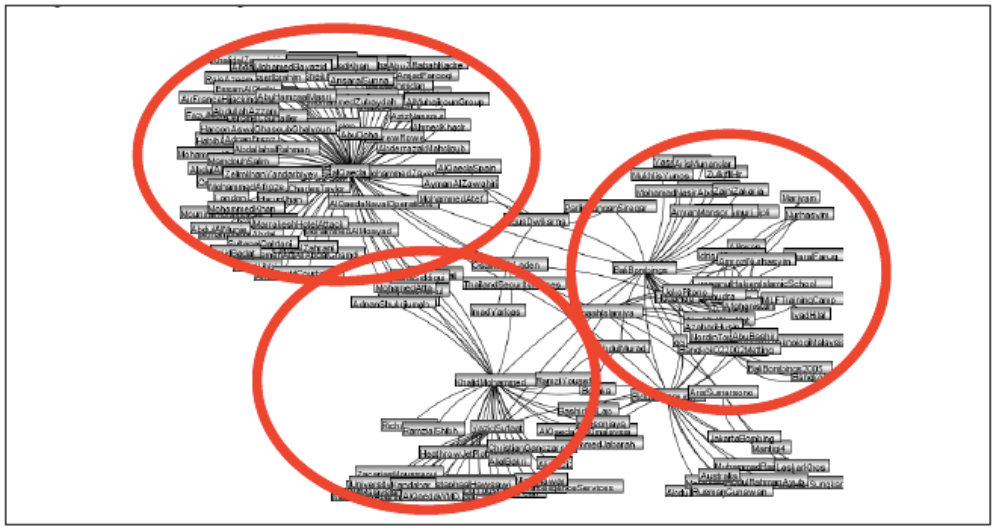
7.2.3.3. TERRORNETVÆRKSANALYSE

Et sidste eksempel på ILP er såkaldt terrornetværksanalyse. Som det blev gjort klart indledningsvist i afhandlingen, så har terror tydeliggjort, at samfund ikke nødvendigvis er sikre. 11/9 2001 er et velkendt eksempel på, hvor omkostningsfuld terror kan være såvel menneskeligt som økonomisk. Forsk-

ning i terror og terror-relaterede emner er steget betydeligt siden 11/9 2001, hvilket ikke er overraskende, idet vi der var vidne til et af de mest skadegørende terrorangreb i historien (Silke, 2008, s. 28). Terror er en af EU's fem sikkerhedstrusler, idet: "[...] it imposes large costs; it seeks to undermine the openness and tolerance of our societies, and it poses a growing strategic threat to the whole of Europe." (Den Europæiske Union, 2003, s. 3).

En måde, hvormed man kan forsøge at bekæmpe terror, er ved analyse af terrornetværk. At lade selve netværket være omdrejningspunkt for terrorbekæmpelse er hensigtsmæssigt, idet det netop er netværket, der er kraftcenteret i terrororganisationer. Dette står i modsætning til mere konventionel krigsførelse, hvor en bestemt lokation har stor betydning og interesse. En lokation eksisterer dog ikke som sådan, når man taler om terror (Wiil, Memon, & Gniadek, 2011, s. 342). Et terrornetværk er grundlæggende et socialt netværk, der dog adskiller sig på forskellige måder fra "almindelige" sociale netværk. Terrornetværk er struktureret specifikt med det formål, at man effektivt skal kunne kommunikere i netværket og dette uden at blive opdaget. (Wiil, Gniadek, Memon, & Petersen, 2013, s. 322).

Et konkret eksempel på et terrornetværk og dets struktur findes i nedenstående visualisering, hvor det netværk, der stod bag terrorangreb på Bali i 2002, er indtegnet.



Billede 20: Visualisering af terrornetværket bag bombeangreb på Bali i 2002 (Wiil, Gniadek, Memon, & Petersen, 2013, s. 332)

Det er en grundlæggende antagelse, når man analyserer terrornetværk, at en forståelse af netværket vil give bedre muligheder for at forhindre kommende terrorangreb. Hvis man har kendskab til et terrornetværk, kan man identificere den eller de centrale personer – også kaldet en knude[196]. Derefter kan man på baggrund af netværkskendskab forsøge at fjerne en eller flere personer med det formål at destabilisere netværket (Wiil, Gniadek, Memon, & Petersen, 2013, s. 322). Kigger man på visualiseringen af terrornetværket, der var involveret i bombeangrebene på Bali, er det overbevisende, at det kan være af afgørende betydning for et terrornetværk, hvis nogle bestemte knuder fjernes. På samme vis er det plausibelt, at fjernelse af andre, mere perifere knuder i netværket vil være uden signifikant betydning for netværkets stabilitet og for kommunikation mellem netværkets medlemmer. En knudes betydning i et netværk er af Wiil et al benævnt *degree centrality*. Jo flere relationer en knude har til andre knuder, desto mere central er denne knude for netværket (Wiil, Gniadek, Memon, & Petersen, 2013, s. 329). *Degree centrality* er et blandt flere forhold, der kan bestemmes med softwaren *CrimeFighter toolbox*, der er et konkret stykke software til at understøtte kortlægning og analyse af terrornetværk (Wiil, Gniadek, Memon, & Petersen, 2013).

[196] Egen oversættelse af "node" (Wiil, Gniadek, Memon, & Petersen, 2013, s. 322).

I *CrimeFighter toolbox* sker analysen af terrornetværk på baggrund af avancerede matematiske modeller og software-værktøjer, hvormed man kan:

> "[...] assist intelligence analyst in harvesting, filtering, storing, managing, analyzing, structuring, mining, interpreting, and visualizing terrorist information." (Wiil, Memon, & Gniadek, 2011, s. 322).

Den grundlæggende antagelse bag *CrimeFighter toolbox* er, at denne software skal hjælpe de personer, der undersøger et netværk, hvilket grundlæggende er en menneskelig opgave (Petersen & Wiil, 2013, s. 2). Dog er dette et så komplekst stykke arbejde, at der er behov for understøttelse af en sådan proces. Ideen med *CrimeFigther toolbox* til understøttelse af en proces er, at man kan modellere knuder og relationerne[197] mellem knuder. En knude kan som nævnt udgøres af en person, men en knude kan også være et sted, en begivenhed eller lignende.

Tidligere har man primært fokuseret på knuder som det væsentligste at kortlægge i forbindelse med modellering af terrornetværk. Antagelsen med *CrimeFighter toolbox* er, at relationerne mellem knuder ligeledes er af væsentlig betydning og samlet set vil bibringe mere viden om et netværk end identifikation af knuder alene ville gøre.

CrimeFighter toolbox består af en række software-pakker: *CrimeFighter Explorer, CrimeFighter Investigator og CrimeFighter Assistant.* Disse softwarepakker indeholder alle *knowledge management* værktøjer, der anvendes i forbindelse med kortlægning og analyse af terrornetværk.

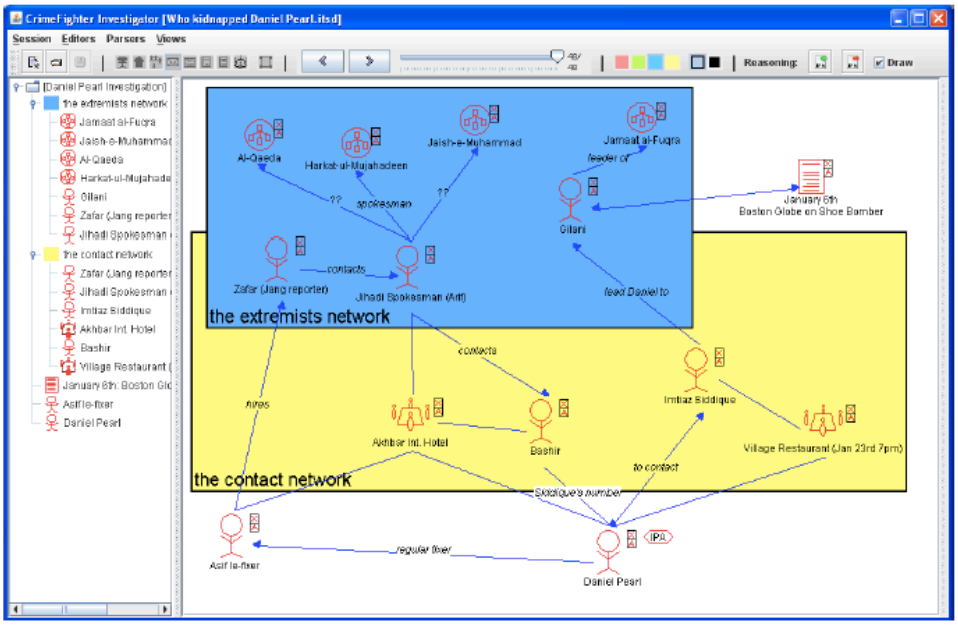
CrimeFighter Explorer bruges til at erhverve data til vidensbasen, også kaldet *knowlegde base* i softwaren. Disse data kan komme fra kilder som for eksempel open source databaser. Data kan ligeledes høstes fra forskellige kilder på internettet. Der kan være tale om data fra sociale medier, fora, blogs, chatrum og lignende. Der kan også være tale om såkaldt *dark web data*. Dark web er de dele af nettet, der ikke bliver indekseret af søgemaskiner såsom Google, AOL

[197] Egen oversættelse af "link" (Wiil, Gniadek, Memon, & Petersen, 2013, s. 322).

og Yahoo. Desuden kan data også komme fra efterretningstjenesters databaser (Wiil, Memon, & Gniadek, 2011, s. 338).

CrimeFighter Investigator anvendes med det formål, at ellers ikke sammenhængende informationer om terror kan sammenfattes i en netværksmodel. Der er med andre ord tale om syntetisering af information, hvilket blandt andet inkluderer opgaver som oprettelse, *editing* og sletning af knuder og relationer. Desuden kan *CrimeFighter Investigator* understøtte meningsskabelse og udtræk af information, der løbende bliver indsamlet ved blandt andet at tillade at arbejde med forskellige hypoteser og forskellige perspektiver på tilgængelig information (Wiil, Gniadek, Memon, & Petersen, 2013, s. 224-226).

Wiil et al demonstrerer, hvordan en kortlægning af et sådan terrornetværk ved brug af *CrimeFighter Investigator* kan se ud i visualisering (billede 21):



Billede 21: Brugergrænseflade på Crimefighter investigator ((Wiil, Gniadek, Memon, & Petersen, 2013, s. 326)

Efter anvendelsen af *CrimeFighter Investigator* til at kortlægge et terrornetværk eller dele heraf kan *CrimeFighter Assistant*-værktøjet anvendes til at understøtte en struktureret analyse af terrornetværk med knuder og relationer samt til visualisering af terrornetværket. Netop det forhold, at forskellige ter-

rornetværk opererer på forskellige måder, ligesom deres formål er forskellige, implicerer, at det ikke er muligt generelt at have én strategi til bekæmpelse af terrornetværk. En analyse af det konkrete terrornetværk er nødvendig, og Wiil et al foreslår, at man blandt andet analyserer effektiviteten af netværket, vigtigheden af de enkelte knuder i netværket, de enkelte knuders roller i netværket og endelig konsekvensen af at fjerne bestemte knuder i forhold til at ødelægge kommunikationsvejene i netværket (Wiil, Gniadek, Memon, & Petersen, 2013, s. 327-330).

Som det er nævnt indledningsvist i dette afsnit, så har terrornetværk visse karakteristika til fælles med sociale netværk, ligesom terrornetværk har visse karakteristika, der er særlige herfor. *CrimeFighter Assistant* kan anvendes til at analysere såvel særlige karakteristika for terrornetværk som generelle netværksforhold. Eksempelvis er *efficiency* et konkret karakteristikum ved et terrornetværk. *Efficiency* er en kvantificering af, hvor effektivt knuder i et netværk kan dele informaiton. Et andet eksempel er *link importance,* der beskriver vigtigheden af en bestemt relation i et netværk. Dette gøres ved at fjerne de konkrete relationer og bestemme, hvorledes det vil påvirke netværket. *CrimeFighter Assistant* kan understøtte besvarelsen af sådanne spørgsmål, hvilket ville være yderst tidskrævende uden understøttende software (Wiil, Gniadek, Memon, & Petersen, 2013, s. 327-330).

Det forekommer overbevisende, at *CrimeFighter toolbox* er et anvendeligt værktøj til at analysere terrornetværk. I lighed med de øvrige eksemplificerede måder at udføre ILP så gør det sig også gældende her, at dele af de data, som er afsæt for analyse af terrornetværk, stammer fra nettet – herunder blogs, chatfora, sociale netværk og lignende. Det er rimeligt at antage, at i hvert fald dele af de data, der finder anvendelse her, ikke er gjort tilgængelige på nettet med henblik på at kvalificere politiets terrorbekæmpelse. Forstås privathed som et kontekstforankret fænomen, får dette svære levevilkår, når brugere, der har gjort data tilgængelige i en anden sammenhæng, pludselig fodrer efterretningstjenester eller politiet med information. Dermed kan der argumenteres for, at man med anvendelse af *CrimeFighter toolbox* løber ind i nogle af de problemstillinger omkring privathed, der er diskuteret i forhold til

environmental scanning og *predictive policing*. Denne diskussion vil ikke blive gentaget her, da problemstillingen for data fra samme eller lignende kilder er behandlet tidligere i afhandlingen.

8. REALISERING AF VÆRDIER I DESIGN

8. REALISERING AF VÆRDIER I DESIGN

Der er tidligere i afhandlingen argumenteret for, at informationel privathed og offentlig sikkerhed begge er værdier, der har signifikant betydning for stat, samfund og individ. Desuden er det påpeget, at det er svært at øge graden af privathed, når et stykke teknologi først er taget i anvendelse (Wang & Kobsa, 2008, s. 18; Klitou, 2014, s. 264). Idet teknologi er bliver mere og mere fremherskende, forekommer det relevant at undersøge og vurdere muligheder for udvikling af etisk forsvarlig teknologi med det formål at undgå at skade individer og øge livskvalitet (van den Hoven, 2007, s. 67). Således må det set i afhandlingens kontekst være relevant at realisere værdien informationel privathed i sikkerhedsteknologi.

I nogle tilfælde bliver teknologi opfattet som en størrelse, der udfordrer vores værdier. Nissenbaum foreslår et modsatrettet perspektiv, hvor der sker en bevægelse *fra værdier til teknologi* (Nissenbaum, 2001, s. 120). Grundlaget herfor er en antagelse om, at værdier påvirker teknologi (Nissenbaum, 2001, s. 120). Såfremt denne antagelse godtages, betyder det også, at det er væsentligt at sikre, at en værdi som informationel privathed understøttes af teknologi. Nissenbaum opfordrer til det, hun kalder *engineering activism*: At man i forbindelse med udvikling af teknologi overvejer, hvilke værdier en teknologi nedarver i dens design, og i de tilfælde, hvor det er muligt, også handler på baggrund heraf (Nissenbaum, 2001, s. 119). VSD og PbD er tilgange, hvormed man kan udføre Nissenbaums *engineering activism* og det, som van den Hoven benævner *front-loading ethics* (van den Hoven, 2007, s. 70). *Front- loading ethics* betoner integrationen af proaktiv, etisk refleksion i design af eksempelvis systemarkitektur (van den Hoven, 2007, s. 70).

VSD er en metodologi til proaktivt at realisere menneskelige værdier i teknologi[198] under hele udviklingsprocessen (Friedman, Kahn, & Borning, 2006;

[198] VSD kan anvendes til udvikling af teknologi forstået mere bredt, men blev i sit udgangspunkt udviklet med fokus på informations- og kommunikationsteknologi (van den Hoven, 2007, s. 68). I nærværende kapitel er diskussionen af VSD og værdibaseret design særligt rettet mod systemer, der kan håndtere data, idet det er den form for sikkerhedsteknologi, som afhandlingen retter sig imod.

Friedman & Kahn, 2003, s. 1186). VSD lægger grundlæggende vægt på et socialt og et etisk ansvar hos dem, der udvikler teknologier. PbD (Cavoukian, 2011) adresserer i modsætning til VSD specifikt værdien privathed. Nødvendigheden af PbD begrundes med teknologiens udvikling, herunder udviklingen af store databaser i netværk (Cavoukian, 2011). Antagelsen er, at privathed ikke kan beskyttes i tilstrækkelig grad ved blot at efterleve krav, som er fastlagt i eksempelvis retskilder. Sikring af privathed i teknologi bør være en del af alle faser i teknologiudvikling (Cavoukian, 2011). Idet VSD og også PbD sigter mod at integrere menneskelige værdier af etiske betydning i design, bliver kriterierne for at bedømme design også bredere end blot et spørgsmål om brugervenlighed og funktionalitet, hvilket er det fokus, der ofte er til stede hos systemudviklere, designere og informationsarkitekter (Friedman & Kahn, 2003, s. 1180; van den Hoven & Manders-Huits, 2012, s. 477-478).

Brugervenlighed er af Friedman og Kahn defineret som: "[...] characteristics of a system that make it work in a functional sense, including that it is easy to usa, easy to learn, consistens, and recovers easily from errors." (Friedman & Kahn, 2003, s. 1180). Friedman et al bemærker, at systemudviklere ofte har ansvar for brugervenlighed, og det er derfor væsentligt, at man i arbejde med VSD er opmærksom på forholdet mellem netop brugervenlighed og etiske værdier, og hvorledes brugervenlighed og etiske værdier i nogle tilfælde kan understøtte hinanden. I andre tilfælde skal brugervenlighed og etiske værdier afvejes i forhold til hinanden (Friedman & Kahn, 2003, s. 1180).

Brugervenlighed er en menneskelig værdi, men ikke en etisk værdi (Friedman & Kahn, 2003, s. 1180). Det er muligt, at brugervenlighed og etiske værdier kan eksistere samtidigt i en teknologi – både afhængigt og uafhængigt af hinanden. En teknologi kan også favorisere brugervenlighed, men samtidigt ikke tillade realisering af etiske værdier. Cookiebekendtgørelsen, der allerede er omtalt og på nuværende tidspunkt gældende, betyder, at man i hvert fald har

haft intentionen om at fremme en etisk værdi som autonomi. Man kan argumentere for, at brugervenligheden i kraft heraf er nedsat.[199]

Formålet med nærværende kapitel er at belyse måder, hvorpå værdier kan realiseres i design med henblik på at nedsætte spændingen mellem informationel privathed og offentlig sikkerhed. I afsnit 8.1., *Value Sensitive Design,* præsenteres og diskuteres VSD indledningsvis i lyset af sikkerhedsteknologi. I de efterfølgende underafsnit behandles en række problemstillinger, der knytter sig til VSD. I afsnit 8.2., *Privacy by Design,* findes en præsentation og diskussion af PbD. Slutteligt i afsnit 8.3., *Vurdering: Værdibaseret design og sikkerhedsteknologi,* er der en samlet vurdering af, om VSD og PbD er anvendelige i forbindelse med udvikling af sikkerhedsteknologi.

De eksempler på sikkerhedsteknologier, som er præsenteret i kapitel 7.2., *Big data som ressource for intelligence-led policing,* vil blive inddraget som diskussionsgrundlag. VSD er en pragmatisk tilgang til at realisere værdier i design, men da nærværende afhandling er et teoretisk projekt, vil jeg ikke slavisk gennemgå, hvordan teorien anvendes i forhold til sikkerhedsteknologi. Det er klart, at de diskussioner, der angår VSD og PbD i forhold til sikkerhedsteknologi, i nogle tilfælde også vil gælde VSD og PbD i relation til andre teknologier.

8.1. VALUE SENSITIVE DESIGN

VSD er en teoretisk funderet metodologi, som kan anvendes til at designe teknologi med henblik på at realisere etiske værdier (Friedman, Kahn, & Borning, 2006, s. 348). Således er VSD også fokuseret på den indflydelse, som teknologien kan have på kvaliteten af menneskers liv (van den Hoven & Manders-Huits, 2012, s. 478).

VSD stammer fra en designtilgang indenfor *human computer interaction*-feltet (herefter blot HCI-feltet) (van den Hoven & Manders-Huits, 2012, s. 477). Her eksisterer også andre tilgange - eksempelvis Computer Supported Cooperative Work (herefter blot CSCW) og Paticipatory Design (herefter blot PA), der

[199] Se dog tidligere diskussion af anvendelsen af informeret samtykke online, hvor jeg stiller spørgsmålstegn ved, om denne praksis medfører et reelt informeret samtykke.

har det fællestræk, at de koncentrerer sig om samarbejde på arbejdspladsen. CSCW sigter oprindeligt mod udvikling af ny teknologi, der kan understøtte samarbejde på arbejdspladsen, men har i dag et bredere fokus, hvor også teknologi, der anvendes i hjemmet, kan tages i betragtning (Friedman & Kahn, 2003, s. 1185). Med udgangspunkt i et ønske om at demokratisere arbejdspladsen har den skandinaviske PA-tilgang formålet at inddrage deltagere i systemudvikling (Friedman & Kahn, 2003, s. 1186). Ifølge social informatik (herefter blot SI), der også eksisterer i HCI-feltet, er det sociale kræfter, der primært former anvendelsen af teknologi (Friedman & Kahn, 2003, s. 1184). Det forhold, at det SI netop antager et instrumentalistisk perspektiv på teknologi betyder, at det kan være problematisk at praktisere for systemudviklere (Friedman & Kahn, 2003, s. 1184-1185; Johnson, 2000, s. 18-19). SI forekommer umiddelbart mest anvendelig til at vurdere en teknologi i anvendelse – SI er således primært et perspektiv og i langt mindre grad en metode (Johnson, 2000, s. 19).

Med afsæt i en demokratisk præmis søger CSCW og PA endvidere hovedsagligt at indlejre funktionelle og instrumentelle værdier i teknologi. I modsætning hertil står VSD, hvis primære fokus er at integrere værdier såsom privathed og autonomi – menneskelige værdier, der er væsentlige fra et etisk perspektiv (van den Hoven & Manders-Huits, 2012, s. 477).

Betegnelsen Value Sensitive Design blev i 1990'erne anvendt til at beskrive en overordnet tilgang til design. Det fælles fundament for Value Sensitive Design-tilgange var, at de fokuserede på menneskelige værdier i teknologi (Davis & Nathan, 2015, s. 11). I dag har Value Sensitive Design ifølge Davis og Nathan (2015) udviklet sig til en term, der udpeger en specifik metodologi (Davis & Nathan, 2015, s. 11-12), og det er netop denne specifikke metodologi, jeg primært vil behandle i nærværende afsnit (Friedman, Kahn, & Borning, 2006; Friedman & Kahn, 2003). Eksempler på andre målrettede tilgange, der fokuserer på værdier i design, er *Values in Design* (Nissenbaum & Gaboury, 2012) og *Values at Play* (herefter blot VaP), hvor sidstnævnte er udviklet specifikt med

henblik på spildesign (Flanagan, Howe, & Nissenbaum, 2005; ValuesAt-Play.org, 2005).[200]

VSD anses for at være den mest omfattende tilgang til at arbejde med menneskelige værdier i teknologi (Albrechtslund, 2007; Le Dantec, Poole, & Wyche, 2009; Manders-Huits, 2011). I afsnit 8.1.1., *Value Sensitive design som metodologi og metode,* beskrives og diskuteres VSD derfor i flere deltaljer.

8.1.1. VALUE SENSITIVE DESIGN SOM METODOLOGI OG METODE

VSD består af en tredelt, iterativ metodologi, hvormed konceptuelle, empiriske og tekniske undersøgelser kan integreres i udvikling af teknologi (Friedman, Kahn, & Borning, 2006; Friedman & Kahn, 2003). Det iterative element i undersøgelserne betyder, at de forskellige undersøgelser ikke nødvendigvis skal optræde i én bestemt rækkefølge eller kun én gang. Formålet med undersøgelserne er, at de skal "informere hinanden" løbende. En lignende ide findes i VaP, hvor metaforen "balls at play" anvendes om de tre undersøgelsesformer, som denne tilgang benytter til realisering af værdier i teknologi. "Ball at play" indikerer, at designerne jonglerer med de tre undersøgelsesformer på relevant vis, imens der sker en dynamisk udvikling af designet (Flanagan, Howe, & Nissenbaum, 2008, s. 325).

De **konceptuelle undersøgelser** udgøres af to sammenhængende dele: En stakeholder-analyse og en konceptualisering og præcisering af menneskelige værdier. Den konceptuelle undersøgelsesfase korresponderer i øvrigt med den designdrejning i anvendt etik, som er omtalt i afhandlingens introduktion. Designdrejningen betoner en mulighed for, at moralfilosofiske analyser kan bringes i spil i forhold til teknologi og dermed bidrage til forandringer i "den rigtige verden" (van den Hoven & Manders-Huits, 2012, s. 479; van den Hoven, 2007).

[200] Der er ikke fuld enighed om, hvorledes forskellige tilgange til værdier i design skal inddeles hierarkisk. For disse forskellige inddelinger se eksempelvis (Nissenbaum & Gaboury, Values In Design, 2012) og (Davis & Nathan, 2015). Jeg tager afsæt i Davis og Nathans (2015) inddeling af tilgange til værdier i design.

Indledningsvis i den konceptuelle fase udpeges direkte og indirekte stakeholders, ligesom det skal bestemmes, hvorledes disse stakeholders påvirkes (Friedman, Kahn, & Borning, 2006, s. 350-351). Direkte stakeholders interagerer direkte med en given teknologi. I modsætning hertil findes de indirekte stakeholders, som ikke interagerer direkte med teknologien, men som stadig bliver påvirket af denne (Friedman, Kahn, & Borning, 2006, s. 350-351, 362-363). I *environmental scanning*-eksemplet, som jeg har inddraget i afsnit 7.2., *Big data som ressource for intelligence-led policing,* kan en indirekte stakeholder i princippet være enhver person, der bidrager med data til det sociale medie, som scannes – i eksemplet i kapitel 7 er der tale om Twitter. En ulempe for en indirekte stakeholder er en potentiel kompromittering af dennes privathed, idet et statsligt organ kan indsamle informationer, som den indirekte stakeholder selv har lagt på et socialt medie. Den direkte stakeholder i dette eksempel er en medarbejder ved en efterretningstjeneste, der gør brug af *environmental scanning*.

Navnlig udpegning af indirekte stakeholders kan give anledning til problemer (Manders-Huits, 2011, s. 277). Her skal det overvejes og bestemmes, hvornår en person er påvirket i en sådan grad, at personen kvalificerer sig til prædikatet indirekte stakeholder.[201] Omvendt må det tages i betragtning, at udpegning af stakeholders er en kontekst-sensitiv opgave, hvorfor det er svært at give præcise anvisninger på, hvordan stakeholders identificeres generelt. Det er heller ikke muligt at fremstille en kvantitativ skala, der angiver, hvornår en person er påvirket i tilstrækkelig grad til at kvalificere sig til benævnelsen indirekte stakeholder. Det må være en vurdering, der skal ske i forbindelse med det enkelte projekt.

[201] En konkret teknik, der kan anvendes til stakeholder-analyse, er brugen af såkaldte *personas* (Friedman, Kahn, & Borning, 2006, s. 363). Personas kan være brugbare til bedre at forstå de fordele og ulemper, der er forbundet med en given teknologi for bestemte stakeholders. Ideen med personas er typisk, at en persona respræsenterer én brugergruppe. Idet forskellige personer kan have en rolle som både indirekte og direkte stakeholder, bør man tillade, at hver persona kan indgå i forskellige grupperinger af stakeholders (Friedman, Kahn, & Borning, 2006, s. 363). Det falder dog uden for afhandlingen at diskutere denne metode nærmere.

Intet hindrer i øvrigt, at en person er både direkte og indirekte stakeholder på samme tid. Man kan forestille sig en person, som arbejder ved Santa Cruz Police Department i Californien, hvor *PredPol* anvendes, men samtidigt bor i det område, hvor der gøres brug af systemet.

Stakeholder-analysen danner en liste med fordele og ulemper for forskellige stakeholders. Disse fordele og ulemper skal nu kortlægges i forhold til korresponderende værdier (Friedman, Kahn, & Borning, 2006, s. 363). Efterfølgende kan værdikonflikter identificeres (Friedman, Kahn, & Borning, 2006, s. 365). En værdikonflikt opstår, når de værdier, der ønskes realiseret i et design, ikke alle kan være til stede på én gang (Flanagan, Howe, & Nissenbaum, 2008, s. 342). Et eksempel kan være en konflikt mellem sikkerhed i et it-system og systemets anvendelighed. Her kan en systemudvikler blive udfordret, idet en høj grad af teknisk sikkerhed kan betyde, at systemet bliver særdeles besværligt at anvende (Flanagan, Howe, & Nissenbaum, 2008, s. 342). Ligeledes kan man mene, at opretholdelse af individers privathed i et it-system kan begrænse et offentligt organs muligheder for overvågning med henblik på at opretholde offentlig sikkerhed. van den Hoven taler i den forbindelse om *moral overload*, hvilket kommer til udtryk, når man er: "[...] burdened by conflicting obligations or conflicting values, which cannot be realized at the same time." (van den Hoven, 2013, s. 77). Moral overload kan i nogle tilfælde afhjælpes ved hjælp af design, hvilket netop er formålet med VSD.

Formålet med VSD er ikke, at en værdikonflikt skal opfattes som en dikotomi, hvor der nødvendigvis skal foretages et valg mellem to eller flere uforenelige værdier. Derimod er formålet at kortlægge mulighederne for, at flere værdier kan realiseres i designet af en teknologi. Friedman et al påpeger dog også, at der vil være uløselige konflikter, og så må den ene værdi have forrang (Friedman, Kahn, & Borning, 2006, s. 365). Der vil med andre ord være tale om en afvejning. VSD kan med hensyn til værdikonflikter opfattes som et værktøj til at træffe et informeret valg, og i nogle tilfælde kan dette valg lede til, at man løser værdikonflikten.

Flanagan et al har i forbindelse med VaP-projektet RAPUNSEL fundet, at tre primære strategier til at arbejde med værdikonflikter blev anvendt (Flanagan, Howe, & Nissenbaum, 2008, s. 342). Formålet med RAPUNSEL-projektet var at udvikle et spilmiljø med henblik på at skabe interesse for IT og lære piger på mellemtrinnet at programmere i programmeringssproget Java (Flanagan, Howe, & Nissenbaum, 2008, s. 331).

Den første strategi benævnes *opløsning af konflikt* og udpeger den situation, hvor der reelt ikke er tale om uforenelige værdier. Derimod er der tale om: "[...] conflicting material constraints that each of the values seemed to impose on the given system or device." (Flanagan, Howe, & Nissenbaum, 2008, s. 343). Et design eller et redesign betyder, at værdikonflikten kan opløses. Et eksempel til illustration af pointen kan være det stykke software til *environmental scanning*, som scanner Twitter, og som er omtalt i afsnit 7.2.3.2., *Environmental scanning af online-ressourcer*. Værdierne offentlig sikkerhed og informationel privathed kan her komme i konflikt, da det forekommer usandsynligt, at personer, der tweeter, primært gør dette med henblik på at fodre politiet eller efterretningstjenester med oplysninger. Disse personer kan opleve, at deres privathed kompromitteres. Værdien sikkerhed er nødvendigvis i spil, idet der er tale om en sikkerhedsteknologi.

Data vil i Nissenbaums terminologi bevæge sig mellem kontekster på en upassende måde og dermed være i konflikt med *normen om distribution af information*. En måde, hvorpå kompromittering af privathed kan undgås i dette eksempel, er ved at sikre, at det enkelte individ aldrig kan identificeres. Data kan i dette eksempel således anonymiseres. Det er givetvis en hensigtsmæssig løsningsmodel i nogle tilfælde, men i andre tilfælde kan et offentligt organ have interesse i at kunne udpege specifikke individer. Der kan også være ønskeligt at få kendskab til bestemte geografiske forhold, hvilket netop er omtalt i *environmental scanning*-eksempelet. Her vil den scanning, der foretages, miste noget af sin værdi, hvis ikke man indsamler data, der kan fastlægge geografiske forhold omkring de neglebarer. I *environmental scanning*-eksemplet indsamles geografiske data konkret ved anvendelse af "location"-tagget (se billede 19).

I de tilfælde, hvor det ikke kan lade sig gøre at designe eller redesigne "sig ud af en værdikonflikt", må der foretages en *afvejning* af de ønskede værdier (Flanagan, Howe, & Nissenbaum, 2008, s. 343). Dette giver muligheden for at træffe et oplyst valg, selvom det ikke nødvendigvis betyder, at alle individer vil kunne erklære sig enige i, at man med en given teknologi har opnået en ønskværdig afvejning af værdier. Om den overvågning af data, der finder sted i Danmark i kraft af Logningsbekendtgørelsen, kan man påstå, at denne netop er et eksempel på, at værdien sikkerhed prioriteres på bekostning af privathed. En sidste mulighed er at indgå et *kompromis.*

På det metodologiske niveau har **empiriske undersøgelser** formålet at undersøge forståelsen, konteksten og oplevelsen hos direkte eller indirekte stakeholders (Friedman & Kahn, 2003, s. 1187). På det metodiske niveau bidrager de empiriske undersøgelser med kvantitative og kvalitative metoder (eksempelvis observation og interviews) med henblik på at koble teknologi til den menneskelige kontekst. I den empiriske undersøgelse inkluderes også verifikation af værdirealisering i teknologi (Flanagan, Howe, & Nissenbaum, 2005, s. 328; Friedman & Kahn, 2003, s. 1187).

Som led i den empiriske undersøgelse kan de, der udvikler et stykke teknologi, interviewe individer, der bor i det område, hvor eksempelvis *PredPol* skal anvendes. Det kan igennem interviews af grupper eller af enkeltpersoner kortlægges, hvordan de indirekte stakeholders anskuer en konkret anvendelse af systemet. Ligeledes kan man på baggrund af nogle opstillede scenarier søge at belyse, om de indirekte stakeholders, der er bosiddende i et bestemt område, opfatter *PredPol* som et redskab, der potentielt kan lede til stigmatisering. Det forekommer dog rimeligt at stille spørgsmålstegn ved, om de implicerede stakeholders reelt er i stand til at tage stilling hertil (Manders-Huits, 2011, s. 278). I eksempelvis *PredPol* indsamles der ikke personhenførebare data, og det kan lede til, at stakeholders konkluderer, at anvendelse heraf er uproblematisk. Men en nærmere diskussion af *PredPol* vil kunne afsløre, at der kan være andre problemstillinger til stede – eksempelvis kan der være tale om, at bestemte områder og dermed også områdernes beboerne kan stigmatiseres og måske også diskrimineres.

Ønsker man at designe teknologi med fokus på privathed, indebærer det også, at der bør eksistere en fælles forståelse af betydningen heraf (Friedman, Hook, Gill, Eidmar, Prien, & Severson, 2008, s. 143). På baggrund af en tværkulturel, empirisk undersøgelse har Friedman påpeget forskelle i forståelsen af værdien privathed i Sverige og USA. I Sverige anvendes om privathed termen "personlig integritet", hvormed både kontrol af informationsflow og kvalitet af data udpeges. I USA refererer "privacy" derimod til informationsflow, men ikke til kvalitet af data (Friedman, Hook, Gill, Eidmar, Prien, & Severson, 2008, s. 143). Forskellige opfattelser af en værdis betydning vanskeliggør en meningsfuld diskussion.

Det er også værd at bemærke, at der ikke nødvendigvis er værdimæssig enighed mellem brugerne og dem, der udvikler et systems værdier. I VaP-projektet RAPUNSEL sondres mellem designernes værdier og brugernes værdier (Flanagan, Howe, & Nissenbaum, 2008, s. 335-338). De kommende brugere af RAPUNSEL fandt det sjovt, at det i spillet var muligt at opbygge karakterer og klæde dem på samt at interagere med andres karakterer (Flanagan, Howe, & Nissenbaum, 2008, s. 336-337). Værdier som ejerskab og kreativ udfoldelse var således vægtet af brugerne. Designerne af RAPUNSEL besluttede, at det skulle være muligt at anvende programmet på andre måder, end de oprindeligt havde tænkt, hvorved værdier som frihed, autonomi og kreativitet fik plads (Flanagan, Howe, & Nissenbaum, 2008, s. 336-338).

Det er uundgåeligt, at en forsker eller en designer vil have indflydelse på et VSD-projekt. En måde at opbløde problemstillingen er, at designeren og forskeren i højere grad skal være tydelige i processen og være eksplicitte vedrørende deres egne værdier (Borning & Muller, 2012, s. 1130; Manders-Huits, 2011; Timmermans & Mittelstadt, 2014, s. 5). Det er væsentligt, at designeren bekender kulør og ikke glimrer ved sit holdningsmæssige fravær. Designeren har signifikant indflydelse på værdier (Flanagan, Howe, & Nissenbaum, 2005, s. 755). Det bliver således gennemskueligt, hvilken rolle designeren spiller. Forskere og designere, der arbejder med VSD-projekter, kan ydermere overveje, om de ikke bør give deres professionelle baggrund til kende i det omfang, det er relevant (Timmermans & Mittelstadt, 2014, s. 5). Borning og Muller

foreslår, at man gennem kommunikation sørger for, at det er tydeligt, hvem der foretager sig hvad (Borning & Muller, 2012, s. 1131).

Endnu et led i den empiriske undersøgelse er verifikation og evaluering af teknologi (Flanagan, Howe, & Nissenbaum, 2008, s. 328). Mary Cummings rejser i den forbindelse et relevant og grundlæggende spørgsmål, nemlig: "How do we know that this human-value centered approach produced a system that is any different or better than if we had not used the VSD approach?" (Cummings, 2006, s. 713). Warnier et al har påpeget, at validering og verificering af privathedsbevarende systemer er et område, der stadig kræver arbejde – hvordan kan man eksempelvis være sikker på, at et givet system sikrer den privathed, vi faktisk ønsker? (Warnier, Dechesne, & Brazier, 2015, s. 443). Ofte vil det ikke være muligt at gennemføre to parallelle designprojekter og efterfølgende foretage en komparativ analyse (Cummings, 2006, s. 713) Det vil være både ressourcekrævende og tidskrævende. Cummings påpeger, at tidligere designprojekter (uden brug af VSD) kan anvendes som sammenligningsgrundlag (Cummings, 2006, s. 713), hvilket er muligt, såfremt et relevant projekt er til rådighed. Det er ikke muligt og ej heller hensigtsmæssigt at fremstille en model for, hvordan en sådan evaluering kan forløbe. Det må afhængige af det enkelte designprojekt.

Formålet med de **tekniske undersøgelser** er at operationalisere værdier i teknologi. Det er også i forbindelse med de tekniske undersøgelser at det bestemmes, i hvilken grad en given teknologi understøtter eller undertrykker bestemte værdier, der er identificeret i forbindelse med konceptuelle og empiriske undersøgelser (Friedman & Kahn, 2003, s. 1187; Friedman, Kahn, & Borning, 2006, s. 351-352). Tekniske undersøgelser kan både fokusere på eksisterende teknologi og på design af ny teknologi.

Uventede værdier og værdikonflikter kan opstå, efter et system er designet og taget i anvendelse. Af den grund er det efterstræbelsesværdigt, såfremt det er muligt, at designe en teknologis arkitektur på en fleksibel måde, således at teknologien kan ændres senere, hvis behovet opstår. Konkret om informationsflow i et systems informationsarkitektur bemærker Friedman et al, at det

skal være muligt at lukke nogle af de protokoller, der frigiver information om personer (Friedman, Kahn, & Borning, 2006, s. 367). Denne betragtning er væsentlig i lyset af, at det er vanskeligt at tilføje privathed til et system, efter at dette er taget i brug (Wang & Kobsa, 2008, s. 18).

Med henblik på at understøtte værdierne informationel privathed og offentlig sikkerhed kunne man eksempelvis undersøge:

- Hvilke informationer de direkte stakeholders, der anvender *environmental scanning,* skal have adgang til.
- Om det er muligt og hensigtsmæssigt at differentiere mellem forskellige brugertyper, så ikke alle har samme adgang.
- Om det er muligt at gøre informationsarkitekturen så tilpas fleksibel, at uforudsete værdikonflikter kan pareres – særligt hvis informationel privathed kommer under pres.

I ovenstående er VSD som metodologi og metode diskuteret og eksemplificeret. I de kommende underafsnit vil jeg diskutere og vurdere mere detaljeret nogle af de spørgsmål, der knytter sig til VSD.

8.1.2. TEKNOLOGI OG VÆRDIER: ET INTERAKTIONSPERSPEKTIV

VSD tager afsæt i et interaktionsperspektiv, der hviler på en antagelse om, at værdier ikke kun kan overføres fra designer til teknologi og ej heller udelukkende er formet af samfundsmæssige forhold og social kontekst (Friedman, Kahn, & Borning, 2006; van den Hoven & Manders-Huits, 2012, s. 478). Derimod påpeges det, at: "[...] the features or proporties that people design into technologies more readily support certain values and hinder others, the technologies actual use depends on on the goals of the people that are interacting with it." (Friedman & Kahn, 2003, s. 1179).

I kraft af interaktionsperspektivet placerer VSD sig imellem teknologideterminisme og instrumentalisme. Teknologideterminisme antager, at et samfunds teknologiske innovationer er drivkraft for udvikling. Når teknologien anvendes, *determinerer* teknologien den menneskelige adfærd og samfundets udvikling (Friedman & Kahn, 2003, s. 1178-1179). Hvis en given teknologi for

alvor får tag i et samfund, bliver det særdeles svært for individet og for samfundet at overskygge de værdier, der drives af denne teknologi.

Det er muligt at argumentere for teknologideterminisme i flere grader, hvoraf den mest vidtgående tilgang foreskriver, at en designer ligefrem kan *overføre* intentioner til en teknologi. Teknologien får således en mental status. En mindre vidtgående version af teknologideterminisme tilsiger, at en teknologi kan kropsliggøre en værdi i en sådan grad, at det kan være svært i en brugssammenhæng at ændre de værdier, som eksisterer i teknologien (Friedman & Kahn, 2003, s. 1178-1179).

VSD tager også afstand fra den antagelse, at samfundsmæssige forhold former teknologi, der i sig selv optræder som et neutralt instrument (Friedman & Kahn, 2003, s. 1179). Teknologi er ifølge denne antagelse hverken et gode eller et onde i sit udgangspunkt, men derimod skyldes konsekvenserne brugen af teknologi. Peter-Paul Verbeek, der i lighed med VSD og PbD har et medierende syn på teknologi, påpeger, at såfremt teknologiske artefakter:

> "[...] are looked at in terms of mediation – how they mediate the relation between humans and their world, amongst human beings, and between humans and technology itself – technologies can no longer be pigeonholed simply as either neutral or determing." (Verbeek, 2005, s. 11).

Den måde, hvorpå man betragter relationen mellem teknologi og menneske, har indflydelse på, hvordan man vil omtale etisk ansvar. Idet man med interaktionsperspektivet antager, at designere og systemudviklere har mulighed for at have en vis indflydelse på teknologien, så gælder det også, at disse netop kan tilskrives et vist ansvar. Spørgsmålet er nu, om det er relevant at designe eller re-designe en teknologi med henblik på realisering af værdier, når man tager afsæt i et interaktionsperspektiv.

VSD søger at designe: "[...] technology that accounts for human values in a principled and comprehensive manner throughout the design process." (Friedman & Kahn, 2003, s. 1186). Albrechtslund har stillet spørgsmålstegn ved præmissen for Friedmans og Kahns udsagn, idet han bemærker, at et sådan udsagn: "[...] rely on the tacit premise that the intentions of carefully designed

technology will correspond with the eventual *use* of technology." (Albrechtslund, 2007, s. 68). Spørgsmålet er dog, om det virkelig er den tavse præmis, som Friedman og Kahn tager udgangspunkt i. Det mener jeg næppe kan være tilfældet, idet VSD tager udgangspunkt i et interaktionsperspektiv. Friedman og Kahns udsagn må således skulle forstås indenfor rækkevidden af interaktionsperspektivet.

Albrechtslund plæderer for nøje at overveje, hvad man som designer rent faktisk har mulighed for at forudsige allerede i designprocessen (Albrechtslund, 2007, s. 68). Det forekommer rimeligt og er en understregning af, at en designer har indskrænket indflydelse på den faktiske anvendelse af teknologi – og det er også det, VSD-tilgangen hævder. Friedman og Kahn gør netop også selv denne pointe eksplicit, idet de skriver om interaktionsperspektivet, at:

> "[...] design and social context matter, dialectically. Moreover, users are not always powerless when faced with unwelcomed value-oriented features of a technology" (Friedman & Kahn, 2003, s. 1180).

En designer kan eksempelvis realisere værdien privathed i et stykke teknologi. Privathed kan understøttes ved, at brugere af et stykke software kun kan tilgå de data, der er nødvendige for, at de kan udføre deres arbejde. Dette kan kontrolleres med et password og vil således give en *kontekstuel integritetstilgang* til privathed (Flanagan, Howe, & Nissenbaum, 2008, s. 327).

Selv når at en given sikkerhedsteknologi er velgennemtænkt fra designers side, så følger det ikke nødvendigvis, at teknologien anvendes som designeren havde forestillet sig. Albrechtslund foreslår her, at designeren søger at adskille intentioner med et design og den faktiske anvendelse (Albrechtslund, 2007, s. 71), hvilket kan siges allerede at ligge implicit i interaktionsperspektivet.

Flanagan et al påpeger ydermere, at det i forbindelse med selve designet kan være nødvendigt at overbevise individer på ledelsesniveau om, at privatheds-beskyttelse er relevant, selv om det måske er fordyrende eller besværliggør visse procedurer (Flanagan, Howe, & Nissenbaum, 2008, s. 327). Utilsigtet anvendelse af et teknologiprodukt vil dog formentlig blive opdaget i forbindelse med en evaluering (Flanagan, Howe, & Nissenbaum, 2008, s. 329). Det er

samtidigt hermed væsentligt, at en designer er bevidst om, hvilken rækkevidde teknologiens design har i forhold til praksis.

8.1.3. VÆRDIER OG HEURISTIK

En værdi er i VSD defineret som: "[...] what a person or group of people consider important in life." (Friedman, Kahn, & Borning, 2006, s. 349).[202] Der er således tale om værdier, der er væsentlige for mennesket. Friedman et al har udarbejdet en liste med tretten for mennesket væsentlige værdier: "[...] human welfare, ownership and proporty, privacy, freedom from bias, universal usability, trust, autonomy, informed consent, accountability, courtesy, identity, calmness, environmental sustainalibilty" (Friedman, Kahn, & Borning, 2006, s. 366). Kendetegnende for disse værdier er, at de er etisk vigtige og ofte implicerede i design af systemer (Friedman, Kahn, & Borning, 2006, s. 349).

De nævnte tretten værdier er en heuristik, der kan anvendes til at give forslag til værdier, der kan implementeres i teknologi (Friedman, Kahn, & Borning, 2006, s. 364). VSD tillader dog, at også andre værdier inkluderes.

Heuristikken skal opfattes som et inspirationskatalog. Spørgsmålet er, om der er en risiko for, at en heuristik kan betyde, at et design af teknologi "skævvrides", idet designere måske vil fokusere på de værdier, som heuristikken stiller til rådighed (Borning & Muller, 2012, s. 1126). Således har Le Dantec et al anført, at en liste med udvalgte værdier kan betyde, at bestemte værdier, der ikke nødvendigvis er i overensstemmelse med de værdier, som stakeholders selv ville have udpeget, fremmes (Le Dantec, Poole, & Wyche, 2009, s. 1142).

Omvendt kan en heuristik være brugbar, idet den kan understøtte, at ingeniører ikke overser relevante værdier (Borning & Muller, 2012, s. 1126). Borning og Muller foreslår brug af kontekstualiserede lister over værdier og betoner samtidig også nødvendigheden af at være eksplicit med hensyn til den kultu-

[202] I litteratur om VSD behandles værdibegrebet ikke indgående, hvilket – kan man hævde - ikke er nødvendigt ud fra en pragmatisk betragtning. Idet jeg netop behandler VSD med denne vinkel, vil jeg ikke diskutere nærmere, hvad der gør, at en størrelse kvalificerer sig til at være en værdi. Ud fra en mere filosofisk betragtning kunne dette være en relevant diskussion.

relle baggrund og det perspektiv, der eksisterer i udviklingen af heuristikken (Borning & Muller, 2012, s. 1126). Samtidigt kan man forestille sig, at VSD ville blive lettere at tilgå for personer uden særlig humanistisk eller filosofisk baggrund, hvis veludviklede værdilister forelå, idet en sådan personkreds vil kunne finde det vanskeligt at begrebsliggøre værdier som autonomi, transparens og privathed. Cummings har netop påpeget, at den konceptuelle undersøgelse sandsynligvis vil være den sværeste for ingeniører at foretage, da det er den mest abstrakte (Cummings, 2006, s. 703). Såvel VSD som VaP lægger dog også op til, at udførsel af projekter skal bygge på en tværfaglig tilgang (Flanagan, Howe, & Nissenbaum, 2008, s. 324-325; Friedman & Kahn, 2003, s. 1186-1187; Nissenbaum, 2001, s. 118-120; van den Hoven, 2007, s. 71).

Idet VSD er en relativt ny metodologi, findes der ikke et utal af *best practice*-eksempler, der kan guide udviklingen indenfor et specifikt område. Der eksisterer dog en række projekter, der kan bidrage til forståelse af og give eksempler på metodologien (se fx (Flanagan, Howe, & Nissenbaum, 2008, s. 327) for RAPUNSEL-projektet eller (Friedman, Kahn, & Borning, 2006) for projektet UrbanSim og cookies i webbrowser, (Friedman, Lin, & Miller, 2005) for projekt om anvendelse af plasma-tv som vindue i kontor, (Xu, Crossler, & Bélanger, 2012) for privathedsværktøjer i webbrowser).

En udpræget praksisnær betragtning kan også være, at mindre virksomheder eller afdelinger i større virksomheder måske ikke har den organisatoriske eller økonomiske kapacitet til at etablere et omfattende VSD-projekt. En heuristik kan her udgøre et brugbart fundament. Borning og Muller har foreslået en mere demokratisk tilgang til udvikling af VSD, hvor flere kan deltage og dele information og erfaring (Borning & Muller, 2012, s. 1132).

8.1.3.1. UNIVERSELLE VÆRDIER I VALUE SENSITIVE DESIGN

VSD tager afsæt i det grundlæggende syn, at der eksisterer universelle værdier, som dog kommer til udtryk på forskellige måder i forskellige kulturer (Friedman & Kahn, 2003, s. 1182-1183; Friedman, Kahn, & Borning, 2006, s. 361). Begrundelsen for at hævde, at værdier er universelle, er empirisk og underbygget af psykologiske og antropologiske data (Friedman, Kahn, & Borning,

2006, s. 361). Hvis man kigger specifikt på værdien privathed, er eksempelvis Alan Westin (1984)[203] kommet til samme konklusion, nemlig at der eksisterer universelle aspekter af denne værdi (Westin, 1984, s. 61).

Westin påpeger blandt andet, at der eksisterer et behov for privathed for individet, familien og for samfundet i alle kulturer. Den funktion, som privathed har, er af afgørende betydning om end forskelligt udtrykt i forskellige kulturer (Westin, 1984, s. 61). Ydermere påpeger Westin, at antropologiske studier viser, at udviklingen fra primitive til moderne samfund har øget de fysiske og psykologiske muligheder for privathed for individ og familie. Industrialisering, urbanisering, individets mulighed for anonymitet i byen og løsrivelsen fra religiøse autoriteter er alle forklaringer herpå (Westin, 1984, s. 69). I lighed med hvad der tidligere i afhandlingen er fremhævet, påpeger Westin, at en række forhold i udviklingen også har haft den modsatte effekt på privathed:

> "[...] density and crowding of populations; large bureaucratic organizational life; popular moods of alienation and insecurity that can lead to desires for new 'total' relations; new instrumnents of physical, psychological, and data surveillance [...] and the modern state, with its military, technological, and propaganda capacities to create and sustain on Orwellian control of life" (Westin, 1984, s. 70).

Som modsætning til det universelle perspektiv på værdier findes den kulturrelativistiske position. Den kulturrelativistiske position hævder, som navnet også antyder, at værdier er kulturbestemte (Rachels & Rachels, 2010, s. 16). Umiddelbart kan kulturel relativisme forekomme tiltalende og som en forklaring på, hvorfor man ikke er enig med andre i deres holdninger til moralske spørgsmål. Ifølge kulturel relativisme eksisterer der ingen universel, moralsk sandhed, og dermed er der heller ikke et grundlag, på hvilket vi kan bedømme andre kulturers handlinger (Rachels & Rachels, 2010, s. 18).

Problemet med den kulturrelativistiske position er, at denne forståelse bygger på et ugyldigt argument (Rachels & Rachels, 2010, s. 18). Personer, der advokerer for kulturel relativisme, påpeger, at forskellige kulturer har forskellige

[203] Originalkilden blev publiceret første gang i 1967.

etiske overbevisninger og moralske koder. På baggrund heraf kan det konkluderes, at der ikke eksisterer en moralsk sandhed. Præmissen, der fremstilles, udpeger, hvad personer *mener*. Konklusionen udpeger, hvad der rent faktisk *er* rigtigt. Men af det forhold, at personer mener, en bestemt handling er rigtig, følger ikke, at det også er rigtigt (Rachels & Rachels, 2010, s. 18). Et håndgribeligt eksempel på denne fejlslutning er, at blot fordi der findes forskellige meninger om, hvorvidt jorden er rund, betyder det ikke, at forskellige konklusioner herom er sande. Kulturel relativisme konkluderer fejlagtigt, at andre kulturer ikke kan tage fejl, og dermed kan man heller ikke tale om, at en kultur kan forbedre sin moral (Rachels & Rachels, 2010, s. 20).

I modsætning til den kulturrelativistiske position repræsenterer den universelle position det synspunkt, at selvom der ses forskellige handlemåder i forskellige samfund, så eksisterer der fælles, grundliggende værdier (Friedman & Kahn, 2003, s. 1182). Der er så at sige nogle værdier, som alle levedygtige samfund må tilslutte sig for at kunne eksistere og fungere. Eksempelvis vil det være problematisk, hvis et samfund ikke lægger vægt på, at man skal tale sandt. Hvis man ikke som udgangspunkt kan antage, at andre taler sandt, så vil kommunikation besværliggøres. Samtidigt er kommunikation en nødvendighed for, at et samfund kan fungere. Det følger heraf, at et samfund må værdsætte en værdi som sandhed (Rachels & Rachels, 2010, s. 20).

Kulturel relativisme kan dog anvendes til at huske os på, at en vis åbenhed overfor andre kulturer er hensigtsmæssig (Rachels & Rachels, 2010, s. 29-30). At hævde at der eksisterer universelle værdier, kan betyde, at nogle grupperinger mener, at de dermed har retten til at påføre andre egne normer og tage midler i brug hertil (Borning & Muller, 2012). Det kan dog blot være et spørgsmål om, at man har tillært sig, at en bestemt praksis er rigtig.

Med en pragmatisk tilgang til VSD vil jeg påpege, at det ikke er strengt nødvendigt at tage stilling til, om værdier er universelle eller kulturelt relative (Borning & Muller, 2012). Måden, man tilgår et fænomen på, vil i høj grad være bestemmende for, hvad man kan konkluderer. Friedman og Kahn eksemplificerer problemstillingen med, at man indenfor hinduismen mener, at enker

bør afholde sig fra at spise fisk, da det vil skade den afdøde persons sjæl, og enken vil lide. Med et vestligt udsyn kan man undre sig over den hinduistiske forståelse, der ikke umiddelbart harmonerer med vestlige overbevisninger. Ovenstående eksempel kan opfattes som et udtryk for divergerende, moralske overbevisninger, hvis man tager afsæt i den kulturrelativistiske position. Omvendt kan eksemplet også netop demonstrere den universelle grundholdning, at man ikke bør skade andre, og man bør øge velfærd (Friedman & Kahn, 2003, s. 1182-1183). Det handler om øjnene, der ser, og måske også hvad man vil se.

Friedman og Kahn anbefaler selv en middelvej som værende er hensigtsmæssig:

> "Theorist who strive to uncover moral universals believe they are wrestling with the essense of morality, with its deepest and most meaningful attributtes. In contrast, theorists who strieve for characterizing moral variation argue that, by the time you have a common moral feature that cuts across cultures, you have so disembodied the idea into an abstract form that it looses virtually all meaning and utility. [...] In our view, both questions have merit, and a middle ground provides a more sensible and powerful approach for the HCI community: One that allows for an analyses of universal moral values, as well as allowing for these values to play out differently in particular culture at a particular point in time." (Friedman & Kahn, 2003, s. 1182-1183).

I et filosofisk perspektiv er det problematisk at ville sidestille ideerne om universelle værdier og relativisme, idet disse antagelser er inkommensurable. Omvendt kan man sige, at det i forhold til en pragmatisk systemudviklingsmetodologi som VSD måske ikke har nogen praktisk betydning. Borning og Kahn giver udtryk for denne holdning, hvilket de kalder en pluralistisk tilgang til værdier:

> "It should be possible for a researcher with a commitment to universel values – or with a commitment to all values being culturally constructed – to employ VSD. In practice, though, we suspect that the answer to this question has little if any impact on most actual projects." (Borning & Muller, 2012, s. 1127).

Flanagan et al anbefaler i lighed hermed, at et pragmatisk kompromis indgås, når der opstår situationer, hvor der mangler svar (Flanagan, Howe, & Nissen-

baum, 2008, s. 326), hvilket er i overensstemmelse med Borning og Muller i citatet ovenfor.

8.1.4. HVIS VÆRDIER I TEKNOLOGI OG MANGLENDE NORMATIV FORANKRING

Et spørgsmål, der knytter sig til VSD, er, hvilken persons eller parts værdier skal fremmes? Denne problemstilling er af afgørende betydning i forhold til afhandlingens problemstilling, idet der her er tale om, at forskellige stakeholders kan have forskellige syn på, hvilke værdier der er væsentlige. Idet VSD ikke har en eksplicit normativ forankring, tilbyder VSD heller ikke en anvisning på, hvorledes værdier skal prioriteres.

NSA's dataindsamling kan tjene som eksempel. Man kan med rette påpege, at værdier allerede er realiseret i XKeyscore, som anvendes af NSA – her er der tale om, at sikkerhed er favoriseret i forhold til privathed (Timmermans & Mittelstadt, 2014, s. 2). VSD kan uden normativt ståsted ikke forhindre, at værdier realiseres på denne måde. Havde VSD en pligtetisk forankring, ville forbuddet mod at anvende individet som middel til at opnå et mål – i dette tilfælde sikkerhed – forhindre realisering af værdien sikkerhed på bekostning af individets privathed.

Spørgsmålet om, hvilken persons eller gruppes værdier der skal fremmes, er også væsentligt for forholdet mellem designer og stakeholders. Der er således ikke nødvendigvis værdisammenfald, når designere og brugere oplister og prioriterer værdier. Desuden kan de, der påvirkes af en teknologi, dvs. de indirekte stakeholders, igen have en anden forståelse af hvilke værdier, der er vigtige.

En bestemt kulturel kontekst kan også være bestemmende for, hvilke værdier der er relevante at fremme. Dette synspunkt er blevet fremstillet af Alsheikh et al (Alsheikh, Rode, & Lindley, 2011), der har udført en empirisk undersøgelse om langdistanceforhold, der er forankret i en arabisk, kulturel kontekst, og implikationerne heraf i forhold til VSD.

Ifølge Alsheikh et al anses individets privathed for værdifuld i den vestlige verden (Alsheikh, Rode, & Lindley, 2011, s. 83). En værdifuld størrelse i ara-

bisk kultur er *ikhilat*, der udpeger konventioner for, hvordan mænd og kvinder må omgås (Alsheikh, Rode, & Lindley, 2011, s. 77). *Ikhilat* er ikke umiddelbart forenelig med en vestlig, feministisk værdi som lighed, og såfremt man ikke er den kulturelle kontekst bevidst, kan man risikere unødigt at påtvinge andre egne værdier. Alsheikh et al har påpeget det væsentlige i at tilgå VSD under hensyntagen til den kulturelle kontekst (Alsheikh, Rode, & Lindley, 2011, s. 83). Friedman et al nævner også, at man skal være den kulturelle baggrund bevidst. Deres perspektiv på værdier inkluderer, som tidligere nævnt, at der eksisterer universelle værdier, men at disse kommer til udtryk på forskellig vis.

Når Friedman et al fremhæver privathed som noget, der: "Refers to a claim, an entitlement, or a right **of an individual** to determine what information about himself or herself can be communicated to others" (min fremhævelse) (Friedman, Kahn, & Borning, 2006, s. 364), skal dette heller ikke opfattes som en ensidig eksemplificering af deres eget vestlige syn på verden. Hvordan værdien privathed konkret kommer til udtryk, vil variere i forskellige kulturer (Friedman, Kahn, & Borning, 2006, s. 361). Privathed opretholdes i en vestlig sammenhæng blandt andet ved hjælp af boligens vægge. I andre kulturer anvendes der andre måder at sikre privathed i en bolig (Friedman, Kahn, & Borning, 2006, s. 361). Det betyder ikke, at privathed ikke er værdifuld her, men privathed kommer blot til udtryk på en anden måde.

VSD hviler som bemærket indledningsvist i nærværende afsnit ikke på en specifik, normativ, etisk teori (Albrechtslund, 2007; Manders-Huits, 2011). Implikationen af den manglende normative forankring er, at VSD kommer til at agere som et etisk neutralt værktøj (Albrechtslund, 2007, s. 68). Albrechtslund spørger i den forbindelse, om VSD kan anvendes som et værktøj til at indlejre: "[...] the ethics and values of, for instance, Nazi Germany?" (Albrechtslund, 2007, s. 67), da tilgangen på nuværende tidspunkt ikke har en præcis og veludviklet måde at definere, hvilke værdier der er tale om. Manders-Huits pointerer i forlængelse heraf, at flere centrale begreber i VSD ikke får nok opmærksomhed og ikke er tilstrækkelig veludviklede, hvilket eksempelvis kan

betyde, at enhver værdi kan have sin berettigelse (Manders-Huits, 2011, s. 280-282).

Ydermere betyder den manglende normative forankring, at prioritering mellem værdier kan være problematisk (Manders-Huits, 2011, s. 283). Det er hensigtsmæssigt at skelne mellem to årsager til denne værdikonflikt. Der kan være tale om en epistemologisk uoverensstemmelse og en ontologisk uoverensstemmelse (Manders-Huits, 2011, s. 283).

Den epistemologiske uoverensstemmelse udpeger menneskers ulige syn på, hvilke værdier der er relevante (Manders-Huits, 2011, s. 283). Disse mennesker, eksempelvis designere af et system, er ikke enige om, hvordan afvejningen af værdier i et system skal ske, fordi de ikke er enige om, hvordan værdierne skal opfattes. Denne problemstilling må dog kunne elimineres, såfremt man i den konceptuelle fase får afklaret værdiernes betydning.

Den ontologiske uoverensstemmelse udpeger værdidilemmaer, hvor man skal foretage en afvejning af værdier (Manders-Huits, 2011, s. 283). Som en følge af det manglende normative ståsted kan VSD ikke være handlingsanvisende med hensyn til, hvordan værdierne skal afvejes. Uden normativt ståsted vil man støde ind i spørgsmålet, om: "[...] who makes the final decision on how to prioritize these competing values?" (Manders-Huits, 2011, s. 283). Med VSD's mangel på normativt ståsted kan metodologien ikke bruges til at begrunde en bestemt prioritering af værdier. VSD forekommer mere anvendelig, hvis der inkluderes et eksplicit, normativt ståsted (Manders-Huits, 2011, s. 283). Hvis VSD eksempelvis tog afsæt i en deontologisk tilgang til normative spørgsmål, ville designprocessen også inkludere tanker om individets ukrænkelighed og ideer om, at man aldrig må bruge individer blot som middel til at opnå et mål. Hvad angår spændingen mellem informationel privathed og offentlig sikkerhed, vil en favorisering af offentlig sikkerhed heller ikke kunne optræde i samme omfang, idet hensynet til individet vil spille en betydningsfuld rolle.

Hvis VSD-metodologien havde et eksplicit, normativt ståsted, kunne VSD opfattes som en operationalisering heraf i forhold til teknologi. Et eksempel herpå findes i medicinsk etik. Bioetikerne Beauchamp og Childress har udledt fire

principper fra den deontologiske grundtanke. De fire principper befinder sig på mellemniveau og benævnes selvbestemmelsesprincippet, lidelses(minimerings)princippet, godheds(maksimerings)princippet og retfærdighedsprincippet (Beauchamp & Childress, 2001, s. 57, 113, 165, 225).[204] Principperne skal anvendes som et redskab for sundhedsprofessionelle til beslutningsstøtte i praksis (Beauchamp & Childress, 2001, s. 23). Principperne giver ikke nødvendigvis en endegyldig løsning eller præcis handleanvisning på etiske problemstillinger, og der kan opstå situationer, hvor principperne kommer i indbyrdes konflikt. Principperne giver dog mulighed for at træffe beslutninger på et oplyst grundlag. På samme måde kan VSD opfattes som en måde at træffe informerede beslutninger vedrørende design af teknologi.

På den ene side kan man argumentere for, at VSD uden normativt ståsted stadig er anvendelig som metodologi, der foreskriver en iterativ proces i forbindelse med et design og realisering af værdier i teknologi. På den anden side kan man hævde, at VSD netop påberåber sig at være en metodologi til design af "normativ teknologi". Hvis man vil fastholde en sådan position, er det problematisk at give køb på at foretage nærmere bestemmelser af det normative ståsted.

VSD's manglende normative ståsted kan løses ved, at man i forbindelse med et konkret VSD-projekt vælger et normativt grundlag for projektet. Den normative teori kan således guide det konkrete projekt og afvejningen af værdier. Her vil det være oplagt at lade overvejelserne i normativ etik være grundlag for afvejning af værdier. Det skal bemærkes, at det er tvivlsomt, om disse teorier kan give entydige svar på, hvordan værdier skal afvejes. Dog kan anvendelsen af teorierne opfattes som en mulighed for beslutningsstøtte, ligesom det gør sig gældende for de omtalte bioetiske principper.

I den nuværende praksis er er der intet, der forhindrer, at man belyser en værdikonflikt med udgangspunkt i flere normative teorier. Man vælger såle-

[204] Principperne er i originalkilden benævnt: "Respect for autonomy", "The principle of nonmaleficence", "Benefience" og "Justice" (Beauchamp & Childress, 2001, s. 57, 113, 165, 225).

des ikke et bestemt normativt ståsted, men flere teorier med henblik på at belyse en problemstilling fra flere vinkler. Hvis man lader flere normative teorier udgøre en form for beslutningsstøtte, er det indlysende, at man ikke vil få et klart svar på, hvordan værdier skal vægtes. Derimod vil dette give anledning til at se en række situationer anskueliggjort fra forskellige sider. På baggrund heraf kan der træffes et valg om, hvordan værdier skal balanceres.

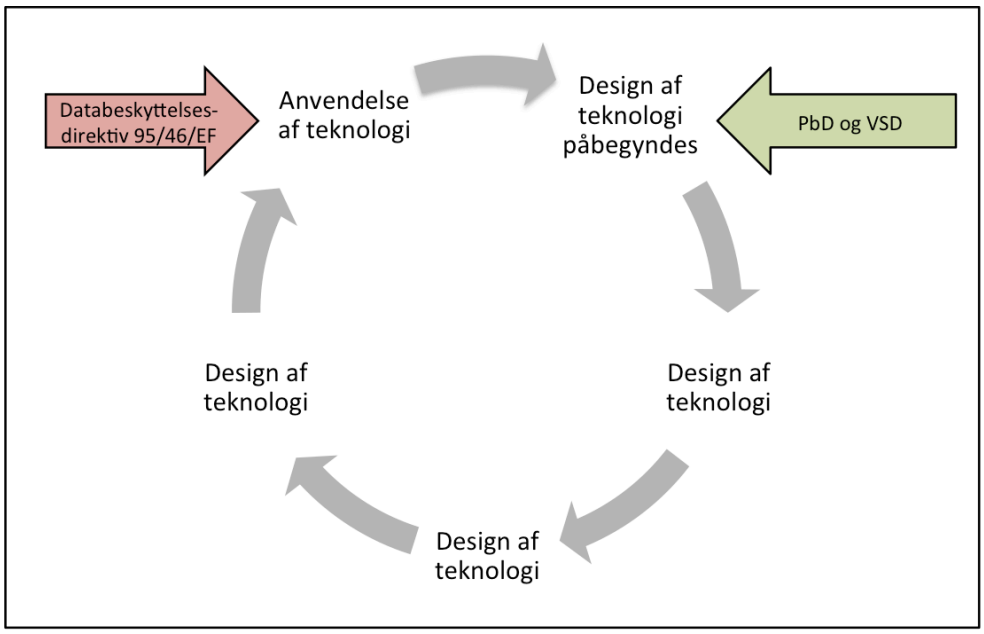
I en medicinsk kontekst har Wulff et al argumenteret for, at når etiske beslutninger skal tages i praksis, så skal overvejelser ske på tre niveauer: Et regelutilitaristisk niveau, et handlingsutilitaristisk niveau og et deontologisk niveau (Wulff, Pedersen, & Rosenberg, 1999, s. 211). De opfordrer således netop til, at man ikke vælger et bestemt, normativt ståsted. I praksis betyder det, at man skal overveje, om man udfører en handling, der har de bedste konsekvenser for patienten, og derudover må man også vurdere konsekvensen, hvis alle handlede på samme måde. Endeligt må man ikke krænke patientens ret til selv at bestemme. Belyses en situation i overensstemmelse med disse retningslinjer, kan der opstå et dilemma (Wulff, Pedersen, & Rosenberg, 1999, s. 211). Anvendelse af flere etiske teorier vil ikke kunne løse enhver værdikonflikt, men designerne vil blive oplyst om, hvad man tilsidesætter, hvis man foretager bestemte valg. Der er således tale om en bevidstgørelse af konsekvenserne ved valg og fravalg.

8.2. PRIVACY BY DESIGN

PbD, der har sikring af privathed som mål, er en helhedsorienteret og proaktiv tilgang, der angår en organisations handlinger, drift og selve it-arkitekturen i et givet system (Cavoukian, 2011; Cavoukian & Chanliau, 2013, s. 9). PbD hviler, som navnet også antyder, på en *design-thinking* opfattelse, hvor privathed inkorporeres i designet af teknologier og systemer (Cavoukian & Chanliau, 2013, s. 2). Den grundlæggende idé bag PbD er, at man skal "bekæmpe" privathedsrelaterede problemstillinger, før de overhovedet opstår (Cavoukian, 2011). PbD skal således ikke opfattes som et tilgang, der benyttes, hvis privathed er blevet kompromitteret, men snarere som en proaktiv foranstaltning, der allerede i udviklingsfasen søger at eliminere krænkelse af privathed.

Hvis man sammenligner PbD med det gældende Databeskyttelsesdirektiv 95/46/EF, så er der en fundamental forskel på, hvorledes man søger at beskytte data. PbD tager afsæt i en antagelse om, at privathed i teknologi ikke udelukkende kan sikres ved reaktivt at efterleve den regulering, der er påkrævet i retskilder. Derfor skal beskyttelse af privathed søges inkorporeret, allerede når design af en teknologi påbegyndes. I modsætning hertil sigter EU's nuværende databeskyttelsesdirektiv mod teknologi i anvendelse.

Forskellen på det nuværende databeskyttelsesdirektiv og ideen i PbD og VSD er illustreret i figur 6.



Figur 6: Databeskyttelsesdirektiv versus PbD/VSD-tilgang.

Databeskyttelseslovgivning er stadig yderst relevant, men beskyttelse af data starter blot tidligere med PbD. Ideen om at inkorporere databeskyttelse i en langt tidligere fase end i forbindelse med anvendelse optræder også i EU's kommende databeskyttelsesforordning (European Commission, 2012, s. art. 23).

I PbD skal privathed realiseres i teknologi ved at efterleve syv grundlæggende designprincipper (Cavoukian, 2011), der har følgende overskrifter:

> "1. ***Proactive*** not Reactive; ***Preventative*** not Remedial

2. Privacy as the ***Default Setting***

3. Privacy ***Embedded*** into Design

4. Full Functionality — ***Positive-Sum***, not Zero-Sum

5. End-to-End Security — ***Full Lifecycle Protection***

6. ***Visibility*** and ***Transparency*** — Keep it ***Open***

7. ***Respect*** for User Privacy — Keep it ***User-Centric***" (Formatering optræder i originalkilde) (Cavoukian, 2011).

Cavoukian anvender termen *zero-sum approach,* hvormed der henvises til ønsket om at opretholde alle legitime interesser. Desuden afviser Cavoukian også såkaldte falske dikotomier såsom privathed versus sikkerhed. Anvendelse af PbD i afhandlingens kontekst betyder således også, at privathed ikke skal "sælges" for sikkerhed. Derimod må offentlige organer som eksempelvis en efterretningstjeneste sørge for at beskytte privathed og sikkerhed (Cavoukian, 2012a, s. 14). I lyset af offentlig sikkerhed og informationel privathed vil en *zero-sum approach* indebære, at hvis en stat opnår mere offentlig sikkerhed, så er det tilladeligt, at individer mister deres privathed – en såkaldt "win/loose"-mentalitet (Cavoukian, 2013, s. 178).

Med hensyn til de sikkerhedsteknologier, der er inddraget i nærværende afhandling, kan softwaredesign, som er udført i overensstemmelse med PbD's principper, eksempelvis sikre, at den enkelte politimand eller person i en efterretningstjeneste aldrig kan få berøring med data, der kan identificere et bestemt individ. Konkret i forhold til det tidligere nævnte *environmental scanning*-eksempel (se afsnit 7.2.3.2., *Environmental scanning af online-ressourcer*) kan man søge at sikre, at man ikke kan genskabe data, der kan udpege enkeltindivider.

Selvom Cavoukian argumenterer for, at man skal undgå falske dikotomier som privathed versus sikkerhed, så forekommer det usandsynligt, at der ikke vil være tidspunkter, hvor det er nødvendigt at give enten privathed eller sikkerhed forrang. Det er ikke en ønskværdig situation, men hvis et hold af ingeniører allerede har forsøgt at opløse en værdikonflikt, og det ikke har været muligt, så må de foretage en afvejning. Det er dog et godt udgangspunkt, at en

værdikonflikt først forsøges løst, og såfremt værdiprioritering bliver nødvendig, sker den afvejning, der foretages, på et oplyst grundlag.

Privathed er ifølge PbD en standardindstilling i et system, og der skal i design af en teknologi som udgangspunkt designes med henblik på maksimal privathedsbeskyttelse (Cavoukian, 2013, s. 181).

Dette PbD-princip flytter ansvaret for at sikre privathed fra brugeren af eksempelvis et socialt medie til ingeniøren. Idet det kan være svært gennemskueligt for den enkelte bruger at vide, hvordan og i hvilken grad brugerens privathed beskyttes, forekommer det rimeligt, at det ikke er den enkelte, der skal sikre sin privathed. Som det er påpeget tidligere i afhandlingen, skal vi således afholde os fra den markedsbaserede tilgang til sikring af privathed, hvor det er op til den enkelte at beskytte egne data. Det kan dog være relevant at skelne mellem forskellige brugertyper. Superbrugere skal have flere muligheder for selv at justere et stykke software end "almindelige brugere". Superbrugere må også forventes at have flere krav og forventninger til, hvad de selv kan kontrollere. I forbindelse med prototypeudvikling af et *Privacy Enhacing Support System* (herefter blot PESS) til en webbrowser foretog Xu et al kvalitative interviews med henblik på evaluering af systemet. Såvel novicer som eksperter blev udspurgt, idet de to brugergrupper ikke nødvendigvis ville have samme forventninger og forbedringsforslag til et PESS (Xu, Crossler, & Bélanger, 2012, s. 428, 431).

Ifølge PbD skal privathedsbeskyttelse af data igangsættes, før man overhovedet er begyndt at indsamle data. Det er også en måde, hvorpå man kan sikre sig, at man ikke ender med at have data til rådighed, som man ikke har behov for. PbD lægger videre vægt på datasikkerhed (Cavoukian, 2011). Manglende sikkerhed ved opbevaring af data kan også bevirke, at privathed kompromitteres.

8.2.1. Problemstillinger ved Privacy by Design-principper i praksis

PbD's syv principper udgør et værktøj, der skal anvendes med henblik på at guide operationalisering af privathed i praksis.[205] Gürses et al har om disse principper påpeget, at det er uklart: "[...] what "privacy by design" actually is and how it should be translated into the engineering practice" (Gürses, Troncoso, & Diaz, 2011). Klitou har på lignende vis betonet, at principperne, der skal guide udvikling, ikke nødvendigvis er specifikke eller detaljerede nok (Klitou, 2014, s. 284). Hvad vil det for eksempel i praksis betyde, at man designer en teknologi med henblik på transparens eller proportionalitet? (Warnier, Dechesne, & Brazier, 2015, s. 439). Warnier et al har mere generelt fremhævet, at der eksisterer en problemstilling, idet de principper, der danner grundlag for design, ofte er vage og abstrakte. Der kan her være tale om både PbD og EU's databeskyttelsesdirektiv (Warnier, Dechesne, & Brazier, 2015, s. 439).

PbD-principperne er udformet som en række grundlæggende principper, der ikke knytter sig til en bestemt teknologi eller kontekst. Ligesom det gælder for VSD, giver PbD ikke lavpraktiske retningslinjer for, hvordan man skal handle i bestemte situationer. Der er derimod tale om en grundlæggende tilgang til, hvordan værdien privathed kan realiseres i design. Warnier et al har påpeget, at når designprincipperne er abstrakte og vage, så tillader man også, at forskellige personer vil opfatte principperne forskelligt (Warnier, Dechesne, & Brazier, 2015, s. 439). En mulighed for at imødekomme denne kritik er, at man udvikler en mere detaljerede designprincipper (Warnier, Dechesne, & Brazier, 2015, s. 439). Til trods for at Warnier et al har en pointe med hensyn til, at det kan være svært at oversætte designprincipper til praksis, finder jeg det ikke hensigtsmæssigt at imødekomme problemstillingen ved at udvikle detaljerede designprincipper. Øger man detaljeringsgraden og tilpasser principperne til bestemt teknologi, nedsætter man samtidig princippernes kontekstuelle uafhængighed.

Det er en styrke, at PbD-principperne er teknologineutrale og kan anvendes i forskellige kontekster. Der forestår et stykke arbejde med at belyse, hvordan

[205] Nogle af de problemstillinger, der gør sig gældende for VSD, gælder også PbD. Jeg vil i tilfælde af sådanne sammenfald ikke tage en næsten identisk diskussion op i forbindelse med PbD.

principperne kan omsættes til praksis i forbindelse med udvikling af teknologi. I takt med at PbD anvendes i forskellige sammenhænge, vil det være muligt for en virksomhed at skele til andres brug heraf, og der vil udvikles en *best pratice*-bank.

En efter min vurdering hensigtsmæssig løsningsmodel er, igen ligesom for VSD, at operere med flere forskellige fagligheder i et PbD-projekt. Det vil give mulighed for, at personer med en humanistisk tilgang til it kan være med til at oversætte principperne, og at personer – eksempelvis systemudviklere – der har de konkrete tekniske kompetencer til at føre principperne ud i praksis, kan forestå den teknisk tunge del af projektet. Det vil stadig være personer med en teknisk baggrund, der skal udføre den tekniske del i praksis, men det vil ske i samspil med personer, der har en humanistisk baggrund. Desuden er det ligesom i et VSD-projekt væsentlig her, at de personer, der udfører et projekt, har en solid forståelse af privathed. Det er trods alt en forudsætning for at kunne vurdere, om privathed overhovedet er indlejret i en teknologi. Dette er endnu et forhold, der taler for, at flere fagligheder er påkrævet i et PbD-projekt.

8.3. VURDERING: VÆRDIBASERET DESIGN OG SIKKERHEDSTEKNOLOGI

Som det netop er demonstreret i de foregående afsnit, knytter der sig en række problemstillinger til VSD og PbD. Der er for VSD tale om udfordringer af mere praktisk karakter – eksempelvis hvorledes man identificerer relevante stakeholders, og hvornår en indirekte stakeholder har tilstrækkelig indflydelse på en given teknologi til netop at kvalificere sig til en sådan betegnelse. PbD-principperne er blevet kritiseret for ikke at være konkrete i en sådan grad, at de kan operationaliseres. Derudover rejser anvendelsen af VSD og PbD også mere grundlæggende, filosofiske problemstillinger såsom spørgsmålet om, hvorvidt der eksisterer universelle værdier, der er delt af alle individer. Flere af de problematikker, som VSD og PbD giver anledning til ved anvendelse i praksis, lader til at kunne imødekommes ved at sikre en tværfaglig

sammensætning blandt dem, der udfører et VSD- eller PbD-projekt, hvilket jeg vil udfolde i nedenstående.

I forhold til afhandlingens ramme giver den manglende normative forankring af VSD anledning til et helt grundlæggende problem: Hvordan skal man vægte værdier? Det er problematisk, at man har en metodologi som VSD, der har til formål at anvise handlinger, men det mere konkrete værktøj til handleanvisning – altså den normative forankring – er ikke ekspliciteret.

Efter min vurdering er der i første omgang tre måder, hvorpå dette problem kan løses: (1) Man kan sammenkoble VSD med et givent normativt ståsted, (2) man kan tillade, at de, der anvender VSD, selv vælger et normativt ståsted, eller (3) man kan anvende forskellige normative ståsteder samtidigt med henblik på at blive oplyst om mulige valg. Disse muligheder er allerede diskuteret i ovenstående.

Yderligere kan en fjerde mulighed være at inddrage en person, der besidder den fornødne etiske ekspertise og viden, og som dermed kan være med til at guide i de forskellige faser ud fra et mere professionelt udsyn. Anvendelsen af en "værdiekspert" kan endvidere være med til at overkomme nogle af de problemer, som stakeholderanalysen kan give. Specifikt hvad angår stakeholders, kan man sætte spørgsmålstegn ved, om "almindelige" mennesker kan gennemskue, hvad konkrete værdier egentlig indeholder, hvad betydningen af at opretholde en værdi som privathed er, eller hvad ulemperne er ved at sætte en sådan værdi under pres.

"Intet at skjule"-argumentet og den diskussion, der knytter sig hertil, er et eksempel på, at stakeholders tilsyneladende har svært ved at overskue kompleksiteten af værdier og ikke mindst værdiers indbyrdes vægtning (Solove, 2007, s. 766). Endnu et eksempel, der kan tjene til at underbygge denne påstand, er egne observationer i forbindelse med undervisning. Studerende har ofte en snæver forståelse af værdien privathed og en klar fornemmelse af, at en værdi som sikkerhed er langt vigtigere. I takt med at undervisningen skrider frem, og de studerende bliver bekendte med forskellige perspektiver på privathed og bevidste om, at privathed refererer til andet end det, der er in-

denfor hjemmets fire vægge, så ændrer deres holdning hertil ofte karakter. De erkender lidt efter lidt privathedsbegrebets kompleksitet.

Det er formentlig en rigelig stor opgave at bede stakeholders, der skal indgå som et led i den empiriske undersøgelse, om at foretage et mindre litteraturstudie af en eller flere værdier forud for et interview. Hvis man trods alt ville anmode stakeholders om det, kan man overveje, om man ikke er bedre stillet med en eller flere professionelle "værdieksperter", der kan være ressourcer i den konceptuelle fase, men også i forbindelse med de øvrige faser.

Anvendelse af værdiekspert i VSD kan dog medføre, at en del af det demokratiske element i metodologien forsvinder. Omvendt kan man overveje, i hvilken grad det demokratisk element er behjælpeligt, hvis de, der skal tage den demokratiske beslutning, ikke besidder den tilstrækkelige viden. Jeg er klar over, at dette argument imod den demokratiske grundtanke er problematisk, idet man lader få, tilstrækkeligt vidende personer have afgørende indflydelse på en beslutningstagning.

En mulighed kan være, at man lader en værdiekspert udføre konceptualisering i den indledende del af et VSD-projekt. Cummings udpeger eksempelvis selv værdien menneskelig velfærd i et VSD-projekt, hvor et missil til den amerikanske flåde udvikles (Cummings, 2006). I den efterfølgende, empiriske undersøgelsesfase kan stakeholders informeres af en værdiekspert og på baggrund heraf tilkendegive deres holdninger. Med denne fremgangsmåde opretholdes det demokratiske princip, hvor man lader ikke-eksperter ytre sig om et givent emne, men også sikrer, at disse ytringer bygger på et informeret grundlag. Anvendelsen af en værdiekspert kan også være med til at afhjælpe problemet om en manglende fælles forståelse af værdier. Hvis stakeholders får fremlagt relevante værdier og uddybende forklaringer af en værdiekspert, så reduceres risikoen for, at den fælles forståelse ikke er til stede.

Ovenstående løsningsforslag medfører, at VSD og PbD trækker på en række fagområder. Hermed sikres dels en fælles forståelse af værdier, dels en sammenkobling mellem funktionelle krav, som systemudviklere tit har fokus på, og etiske værdier, som VSD og PbD fordrer. Cummings skriver i den forbindel-

se, at det vil være problematisk at overlade den konceptuelle fase til systemudviklere (Cummings, 2006). Personer med en større humanistisk indsigt skal derfor involveres i udvikling af it-systemer.

Såvel VSD som PbD lægger op til, at værdier i design skal tilgås proaktivt (Cavoukian, 2011; Friedman & Kahn, 2003; Nissenbaum, 2001; van den Hoven, 2007). Herved nedsættes risikoen for at udvikle en teknologi, som senere viser sig at have uhensigtsmæssige konsekvenser. Det betyder omvendt ikke, at der ikke kan udvikles sikkerhedsteknologi, der sætter privathed under pres og favoriserer offentlig sikkerhed. Men det forekommer rimeligt at antage, at såfremt dette alligevel sker, så er beslutningerne herom truffet på et oplyst grundlag. Jeg anser det at træffe oplyste valg og fravalg for at være langt mere hensigtsmæssigt end at fravælge eksempelvis privathed uden at være bevidst om implikationer heraf. Det medfører dog, at man i forbindelse med anvendelsen af værdibaseret design er bevidst om rækkevidden af disse metoder. Både VSD og PbD skal forstås med afsæt i et interaktionsperspektiv.

For såvel VSD og PbD gælder det endvidere, at der er tale om tilgange til design, der er kontekstuafhængige og uafhængige af teknologi. Der har været rettet en kritik mod tilgangene af selv samme grund (Gürses, Troncoso, & Diaz, 2011; Klitou, 2014; Warnier, Dechesne, & Brazier, 2015). PbD er dog tænkt som en række grundlæggende og generelle principper, der skal kunne anvendes i forhold til en bredt spektrum af informationsteknologier. At anvende VSD vil ligeledes kræve, at man kan forankre metodologien i det enkelte projekt, da denne i sit udgangspunkt er mere generel.

Ovenstående problemstilling med at "oversætte" PbD og VSD til et konkret projekt kan imødekommes ved at lade personer med forskellige, faglige kompetencer samarbejde (Cummings, 2006, s. 714; Flanagan, Howe, & Nissenbaum, 2008, s. 324). Særligt i forbindelse med konceptualisering af værdier vil en humanist have sin styrke og kunne bidrage med begrebsliggørelse af en værdi som privathed. Individer med en humanistisk baggrund vil tillige kunne hjælpe med at oversætte PbD-principperne til det konkrete projekt.

9. KONKLUSION

9. KONKLUSION

Formålet med afhandlingen er dels at undersøge den spænding, der er mellem værdierne informationel privathed og offentligt sikkerhed, når sikkerhedsteknologier anvendes af staten, dels at vurdere om udvalgte værdibaserede designtilgange kan anvendes til at realisere værdier i teknologi.

Det er ved hjælp af eksempler illustreret, at problemstillingen er relevant og aktuel i den samtid, vi lever i. Stater indsamler og overvåger information med henblik på at øge den offentlige sikkerhed. En række sikkerhedspolitiske tiltag, der er iværksat efter 11/9 2011, er desuden præsenteret og diskuteret med henblik på at rammesætte problemstillingen. Den dataindsamling, der sker i henhold til Logningsbekendtgørelsen, og NSA's overvågning har gennem afhandlingen tjent om eksempler på konkret overvågning. Problemstillingen, informationel privathed versus offentlig sikkerhed, optræder endvidere jævnligt i den offentlige debat og er interessant at behandle, da den har berøring med og betydning for "helt almindelige mennesker".

Kernen i afhandlingen har været den spænding, der eksisterer mellem værdierne informationel privathed og offentlig sikkerhed. Spændingen opstår, når starter overvåger borgere ved hjælp af de data, der eksisterer om individer, og som i nogle tilfælde gøres tilgængelige online af selv samme individer. Hovedparten af afhandlingens kapitler har haft som omdrejningspunkt at behandle forskellige elementer, der knytter sig til denne spænding.

Det er demonstreret på baggrund af en teoretisk diskussion, at det er problematisk for stat, samfund og individ, hvis der ikke gives plads til, at værdien informationel privathed kan opretholdes. Således er ideen i den utilitaristiske nyttetanke, nemlig at det er en gevinst for de mange, at sætte privathed under pres med henblik på at øge sikkerhed, også udfordret. Ydermere er det i forhold til værdien informationel privathed – og privathed mere generelt – påpeget, at nogle af de anomalier, man kan se i forhold til privathed, kan forklares med en kontekstuel forståelse af privathed. Den uoverensstemmelse, som tilsyneladende eksisterer mellem den voksende interesse for privathed og det

forhold, at mange mennesker gør information om dem selv frit tilgængelig på internettet, er med en kontekstuel opfattelse af privathed gjort forståelig.

En central pointe i afhandlingen er, at privathed ikke alene er vigtig for individet, men i høj grad også for samfundet og for staten. Det liberale demokrati har behov for privathed, det politiske virke har behov for privathed, og det er en forudsætning for valghandlinger, at der er privathed. Det er sandsynliggjort, at privathed i et etisk perspektiv er væsentligt at behandle. Der eksisterer – navnlig i EU - en omfattende mængde retskilder, der sikrer beskyttelse af data. Disse retskilder kan betragtes som en nødvendig, men ikke tilstrækkelig betingelse for informationel privathed. Etisk forsvarlighed indenfor området er også nødvendig.

Værdien af offentlig sikkerhed er behandlet, ligesom den ontologiske relation mellem stat og borger er præciseret i forhold til afhandlingens ramme. Det er her demonstreret, at det ikke er tilstrækkeligt at tale om sikkerhed som en værdi, der udelukkende knytter an til staten. Individets sikkerhed er ligeledes væsentlig, idet statens sikkerhed ikke nødvendigvis implicerer individets sikkerhed.

Konkret er der i afhandlingen inddraget tre sikkerhedsteknologier, der alle kan anvendes til at overvåge data. Sikkerhedsteknologierne kan anvendes med henblik på at nedsætte henholdsvis terror eller organiseret kriminalitet, hvilket er to af EU's fem nøgletrusler i seneste sikkerhedsstrategi fra 2003. Sikkerhedsteknologierne optræder i afhandlingen som scenarier, hvis funktion er dels at eksemplificere en mulig anvendelse, dels at udgøre et teoretisk diskussionsgrundlag og illustrere pointer.

Med et pragmatisk afsæt har jeg diskuteret VSD's og PbD's anvendelsesmuligheder i forhold til sikkerhedsteknologi. Det er påpeget, at disse tilgange er anvendelige, om end der knytter sig problemstillinger hertil. Problemstillingerne spænder vidt i omfang og karakter. Nogle af problemstillingerne er særdeles betydningsfulde og bunder i omfattende filosofiske problemer – eksempelvis spørgsmålet om hvorvidt værdier er universelle. Det er klart, at det ikke er muligt at løse et sådant problem i nærværende afhandling. Derimod er

det formålstjenligt at anvise en pragmatisk løsningsmodel, ligesom diskussionen af problemstillinger vedrørende VSD og PbD lægger op til videre forskning indenfor dette område.

Det er også min forhåbning, at brugen af VSD og PbD kan vinde indpas i sikkerhedsteknologi. Det er tale om en metodologi og en række grundlæggende principper, der allerede finder anvendelse. På baggrund af diskussion og vurdering skønner jeg, at disse tilgange er brugbare, omend der er rum for udvikling og forbedring. Anvendelsen af VSD og PbD vil også kunne bidrage til, at de forfines og til at øge massen af tilgængelige projekter i en "*best practise* projektbank". Ydermere er det påpeget, at anvendelse af tværfaglighed i projekterne vil imødekomme nogle af de problemstillinger, som tilgangene møder i praksis.

I en mere "populær formidlingskontekst" kan min forhåbning være, at afhandlingens demonstration af, at privathed er af signifikant betydning for stat, samfund og individ, kan give nyt liv til diskussionen om, i hvilken grad stater bør overvåge individer. Uden at have foretaget en systematisk analyse af udsagn i den offentlige debat, forekommer det mig, at der ofte diskuteres på baggrund af forudsætninger, der ikke er forenelige med det, som jeg i afhandlingen er argumenteret for. I den offentlige debat er det sjældent at udfordre ideen om, at sikkerhed er et gode for de mange og manglen på privathed er udelukkende individet tab. Hvis stat, samfund og individ alle kan drage fordel af at opretholde offentlig sikkerhed og informationel privathed, må man antage, at omfanget og måden, hvorpå man overvåger data, vil blive genovervejet.

10. LITTERATUR

10. LITTERATUR

Albrechtslund, A. (maj 2008). *In the Eyes of the Beholder. Introducing participation and ethics to surveillance* , 1-66. Aalborg, Danmark: Institut for kommunikation, Aalborg Universitet.

Albrechtslund, A. (2007). Ethics and technology design. *Ethics and Information Technology , 9* (1), s. 63-72.

Allen, A. L. (2011). *Unpopular Privacy: What Must We Hide?* New York, New York, USA: Oxford University Press.

Al-Saggaf, Y., & Islam, M. Z. (12. June 2014). Data Mining and Privacy of Social Network Sites' Users: Implications of the Data Mining Problem. *Science and Engineering Ethics , 21* (4), s. 941-966.

Alsheikh, T., Rode, J. A., & Lindley, S. E. (2011). (Whose) Value-Sensitive Design? A Study og Long-Distance Relationships in an Arabic Cultural Context. *Proceedings of the ACM 2011 conference on computer supported cooperative work* , s. 75-84.

Anderson, C. (26. juni 2008). *wired.com, The End of Theory: The Data Deluge Makes the Scientific Method Obsolete*. Hentede 19. august 2014 fra wired.com: archive.wired.com/science/discoveries/magazine/16-07/pb_theory

Aquilina, K. (march 2010). Public security versus privacy in technology law: A balancing act? *Computer Law and Security Review: The International Journal of Technology and Practice , 26* (2), s. 130-143.

ARTICLE 29 Data Protection Working Party. (1. december 2009). *ec.europa.eu, The Future of Privacy*. Hentede 15. august 2015 fra ec.europa.eu: ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2009/wp168_en.pdf

ARTICLE 29 Data Protection Working Party. (10. april 2014). *Opinion 04/2014 on surveillance of electronic communications for intelligence and national security purposes.* Hentede 31. august 2015 fra ec.europa.eu:

ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp215_en.pdf

Ayer, A. J. (1990). *Language, Truth and Logic.* London, England: Pinguin Books.

Bacher, J. (2013). *Predictive Policing: Preventing Crime with Data and Analytics.* Improving Performance Series, IBM Center for The Business of Government, Washington D.C.

Ball, K., Lyon, D., Wood, D. M., Norris, C., & Raab, C. (September 2006). *A Report on the Surveillance Society. For the Information Commissioner by the Surveillance Studies Network. Full Report* . (D. M. Wood, Red.)

Barbaro, M., & Zeller, T. (9. August 2006). *the New York Times, A Face Is Exposed for AOL Searcher No. 4417749*. Hentede 3. November 2014 fra nytimes.com: nytimes.com/2006/08/09/technology/09aol.html?pagewanted=all&_r=0

Bauer, F., & Kaltenböck, M. *Linked Open Data: The Essentials. A Quick Start Guide for Decision Makers.* Vienna, Austria.

Beauchamp, T. L., & Childress, J. F. (2001). *Principles of biomedical ethics* (5. udg.). New York, New York, USA: Oxford University Press.

Beken, T. V. (2004). Risky business: A risk-based methodology to measure organized crime. (M. Levi, Red.) *Crime, Law & Sociale Change , 41* (5), s. 471-516.

Benn, S. I. (1984). Privacy, freedom, and respect for persons. I F. D. Schoeman (Red.), *Philosophical Dimensions of Privacy: An Anthology* (s. 223-244). Cambridge University Press.

Bentham, J. (2007). *An Introduction to the Principles of Morals and Leglislation* (1. udgave udg.). Mineola, New York, USA: Dover Publications.

Bentham, J. (1843). *The Works of Jeremy Bentham. Panopticon, or, the Inspection-House, & c.* (J. Bowring, Red.)

Biehn, N. (5. June 2013). *wired.com, The Missing V's in Big Data: Viability and Value*. Hentede 8. august 2014 fra Wired.com: wired.com/2013/05/the-missing-vs-in-big-data-viability-and-value/

Blume, P. (2000). To foredrag om integritet, privatliv og samfund. *Retsvidenskabeligt Institut B* , 1-41. Københavns Universitet.

Bollier, D. (2010). *The Promise and Peril of Big Data.* The Aspen Institute , Communications and Society Program. Washington D.C: The Aspen Institute .

Borning, A., & Muller, M. (2012). Next Steps for Value Sensitive Design. *Proceedings of the 2012 ACM annual conference on human factores in computing systems* , s. 1125-1134.

boyd, d., & Crawford, K. (15. June 2012). CRITICAL QUESTIONS FOR BIG DATA Provocations for a cultural, technological, and scholarly phenomenon. *Information, Communication & Society , 15* (5), s. 662-679.

Branco, P. (2010). On Prisons and Theatres: Santo Stefano and San Carlo. *Law Text Culture , 14* (15), s. 277-285.

Brewster, B., Akhgar, B., Staniforth, A., Waddington, D., Andrews A., Mitchell, S., et al. (2014a). Towards a model for the integration of knowledge management in law enforcement agencies. *International Journal of Electronic Security and Digital Forensics , 6* (1), s. 1-17.

Brewster, B., Polovina, S., Rankin, G., & Andrews, S. (2014b). Knowledge Management and Human Trafficking: Using Conceptual Knowledge Representation, Text Analytics and Open-Source Data to Combat Organized Crime. (N. Hernandez, R. Jäschke, & M. Cro, Red.) *Graph-Based Representation and Reasoning: 21st International Conference on Conceptual Structures, ICCS 2014, Iaşi, Romania, July 27-30, 2014, Proceedings* , s. 104-117.

Cavoukian, A. (2012a). *Abandon Zero-Sum, Simplistic either/or Solutions - Positive-Sum is Paramount: Achieving Public safety and Privacy.* Ontario: Information and Privacy Commissioner.

Cavoukian, A. (1998). *Data Mining: Staking a Claim on Your Privacy.* Ontario: Information and Privacy Commissioner.

Cavoukian, A. (2012b). *Operationalizing Privacy by Design: A Guide to Implementing A Strong Privacy Practices.* Ontario: Information and Privacy Commissioner.

Cavoukian, A. (2011). *Privacy By Design - The 7 Foundational Principles.* Ontario: Information and Privacy Commissioner.

Cavoukian, A. (2012c). *Privacy by Design from Rhetoric to Reality.* Ontario: Information and Privacy Commissioner.

Cavoukian, A. (2013). Privacy by Design: Leadership, Methods, and Results. I S. Gutwirth, R. Leenes, P. de Hert, & Y. Poullet, *European Data Protection: Coming of Age* (1. udg., s. 175-202). Springer Netherlands.

Cavoukian, A., & Chanliau, M. (2013). *Privacy and Security by Design: A Convergence of Paradigms.* Ontario: Information and Privacy Commissioner.

Cavoukian, A., Stewart, D., & Dewitt, B. (2014). *Using Privacy by Design to Achieve Big Data Innovation Without Compromising Privacy.* Ontario: Information and Privacy Commissioner, Deloitte.

Chen, H., Atabakhsh, H., Tseng, C., Marshall, B., Kaza, S., Eggers, S., et al. (april 2005). Visualization in Law Enforcement. *CHI '05 Extended Abstracts on human factors in computing systems* , s. 1268-1271.

Choo, C. W. (februar 1999). The art of scanning the environment. *American Society for Information Science. Bulletin of the American Society for Information Science , 25* (3), s. 21-24.

Clarke, R. (1993a). *CFP'93 - Computer Matching and Digital Identity.* Hentede 16. januar 2014 fra www3.nd.edu: www3.nd.edu/~mgrecon/datafiles/articles/computermatching.html

Clarke, R. (maj 1988). Information Technology and Dataveillance. *Communications of the ACM , 31* (5), s. 498-512.

Clarke, R. (december 1993b). Profiling: A Hidden Challenge to the Regulation of Data Surveillance. *Journal of Law and Information Science , 4* (2), s. 403-419.

Clarke, R. (oktober 2013). *rogerclarke.com, Introduction to Dataveillance and Information Privacy, and Definitions of Terms*. Hentede 14. februar 2014 fra rogerclarke.com: rogerclarke.com/DV/Intro.html

Commission on Human Security. (2003). *Human Security Now.* United Nations, New York.

Cope, N. (marts 2004). Intelligence led policing or policing led intelligence? Integrating Volume Crime Analysis into Policing. *The British Journal of Criminology , 44* (2), s. 188-203.

Craig, T., & Ludloff, M. E. (2011). *Privacy and Big Data.* U.S.A: O´Reilly.

Cummings, M. L. (2006). Integrating Ethics in Design through the Value-Sensitive Design Approach. *Science and Engineering Ethics , 12* (4), s. 701-715.

Datatilsynet. (u.d.). *datatilsynet.dk, Biometri*. Hentede 12. februar 2015 fra datatilsynet.dk: datatilsynet.dk/borger/biometri/

Davis, J., & Nathan, L. P. (2015). Value Sensitive Design: Applications, Adaptions, and Critiques. I J. van den Hoven, P. E. Vermaas, & I. van de Poel (Red.), *Handbook of Ethics, Values, and Technological Design. Sources, Theory, Values and Application Domains* (1. udgave udg., s. 11-40). Springer Netherlands.

De Forenede Nationer. (10. december 1948). *menneskeret.dk, Verdenserklæringen om Menneskerettighederne.* Hentede 27. maj 2015 fra menneskeret.dk: menneskeret.dk/files/media/dokumenter/om_os/om_menneskerettigheder_diverse/fn_verdenserklaering.pdf

De Hert, P. (September 2005). Balancing security and liberty within the European human rights framework. A critical reading of the Court's case law

in the light of surveillance and criminal law enforcement strategies after 9/11. *Utrecht Law Review , 1* (1), s. 68-96.

DeCew, J. (9. august 2013). *plato.stanford.edu, The Stanford Encyclopedia of Philosophy, privacy*. (E. N. Zalta, Redaktør) Hentede 2. marts 2015 fra plato.stanford.edu: plato.stanford.edu/archives/spr2015/entries/privacy/

Dechesne, F., Warnier, M., & van den Hoven, J. (september 2013). Ethical requirements for reconfigurable sensor technology: a challenge for value sensitive design. *Ethics and Information Technology , 15* (3), s. 173-181.

Den Europæiske Union. (12. december 2003). *consilium.europa.eu, A Secure Europe in a Better World. European Security Strategy.* Hentede 27. februar 2015 fra consilium.europa.eu: consilium.europa.eu/uedocs/cmsUpload/78367.pdf

Den Europæiske Union. (31. januar 2005). *eur-lex.europa.eu, Traktat om en forfatning for Europa.* Hentede 2. august 2015 fra eur-lex.europa.eu: eur-lex.europa.eu/legal-content/DA/TXT/PDF/?uri=OJ:C:2004:310:FULL&from=DA

Den Europæiske Union. (10. Oktober 2010). *europarl.europa.eu, Den Europæiske Unions Charter om Grundlæggende Rettigheder.* Hentede 27. februar 2015 fra europarl.europa.eu: europarl.europa.eu/charter/pdf/text_da.pdf

Den Store Danske. (u.d.). *denstoredanske.dk, Corporate Social Responsibility*. Hentede 22. september 2012 fra denstoredanske.dk: denstoredanske.dk/Erhverv,_karriere_og_ledelse/Erhvervsliv/Management/corporate_social_responsibility

Department of Homeland Security. (23. juli 2012). *dhs.gov, Homeland Security Act of 2002*. Hentede 4. marts 2015 fra dhs.gov: dhs.gov/homeland-security-act-2002

Det Europæiske Råd. (4. maj 2010). *eur-lex.europa.eu, DET EUROPÆISKE RÅD-STOCKHOLMPROGRAMMET — ET ÅBENT OG SIKKERT EUROPA BORGERNES*

TJENESTE OG TIL DERES BESKYTTELSE. Hentet fra eur-lex.europa.eu: eur-lex.europa.eu/legal-content/DA/TXT/PDF/?uri=CELEX:52010XG0504(01)&from=DA

Digitaliseringsstyrelsen. (22. april 2013). *digst.dk, Open Data Innovation Strategy (ODIS)*. Hentede 29. april 2014 fra digst.dk: digst.dk/Servicemenu/English/Policy-and-Strategy/Open-Data-Innovation-Strategy-ODIS.aspx

Dwork, C., & Mulligan, D. K. (3. September 2013). It's Not Privacy, and It's Not Fair. *Stanford Law Review Online , 66*, s. 35-40.

Dyer, C. (1. januar 2002). *theguardian.com, Woolf admits concern at new detention law*. Hentede 10. juli 2014 fra theguardian.com: theguardian.com/uk/2002/jan/01/politics.september11

Edgar, S. L. (2002). Privacy. I S. L. Edgar, *Morality and Machines: Perspectives on Computer Ethics* (2. udg.). USA: Jones and Bartlett Publishers.

Electronic Privacy Information Center. (2015). *EPIC.org, The Privacy Act of 1974*. Hentede 23. marts 2015 fra EPIC.org: epic.org/privacy/1974act/

Erhvervsstyrelsen. (april 2013). *erhvervsstyrelsen.dk, Vejledning til bekendtgørelse om krav til information og samtykke ved lagring af eller adgang til oplysninger i slutbrugerens terminaludstyr, "Cookie-bekendtgørelsen".* Hentede 14. august 2015 fra erhvervsstyrelsen.dk: erhvervsstyrelsen.dk/sites/default/files/vejledning-cookiebekendtgorelse.pdf

Ericson, R. V., & Haggerty, K. D. (1997). *Policing the risk society.* Oxford: Clarendon Press.

Ess, C. (2009). *Digital Media Ethics* (1. udg.). Storbritannien: Polity Press.

EU-Oplysningen. (u.d.). *eu.dk, Hvad er EU's terrordefinition?* Hentede 18. maj 2015 fra eu.dk: eu.dk/da/spoergsmaal-og-svar-folder/hvad-er-eus-terrordefinition

Europa-parlamentet og rådets direktiv. (24. oktober 1995). *95/46/EF, om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger.* Hentede 2. april 2014 fra eur-lex.europa.eu: eur-lex.europa.eu/legal-content/DA/TXT/PDF/?uri=CELEX:31995L0046&from=DA

Europa-Parlamentets og rådet. (25. november 2009). *2009/136/EF, om ændring af direktiv 2002/22/EF om forsyningspligt og brugerrettigheder i forbindelse med elektroniske kommunikationsnet og -tjenester, direktiv 2002/58/EF om behandling af personoplysninger og beskyttelse af privatlivets fred i den elektroniske kommunikationssektor og forordning (EF) nr. 2006/2004 om samarbejde mellem nationale myndigheder med ansvar for håndhævelse af lovgivning om forbrugerbeskyttelse.* Hentede 28. maj 2015 fra eur-lex.europa.eu: eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:0036:da:PDF

Europa-parlamentets og rådets direktiv. (15. marts 2006). *2006/24/EF, om lagring af data genereret eller behandlet i forbindelse med tilvejebringelse af offentligt tilgængelige elektroniske kommunikationstjenester eller elektroniske kommunikationsnet og om ændring af direktiv 2002/58/EF.* Hentede 27. februar 2015 fra eur-lex.europa.eu: eur-lex.europa.eu/legal-content/DA/TXT/PDF/?uri=CELEX:32006L0024&qid=1425027464238&from=DA

Europa-parlamentets og rådets direktiv. (12. juli 2002). *Direktiv 2002/58/EF, om behandling af personoplysninger og beskyttelse af privatlivets fred i den elektroniske kommu- nikationssektor (Direktiv om databeskyttelse inden for elektronisk kommunikation).* Hentede 27. februar 2015 fra eur-lex.europa.eu: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:201:0037:0047:da:PDF

Europa-Parlementets og rådets direktiv. (2011). *2011/36/EU, om forebyggelse og bekæmpelse af menneskehandel og beskyttelse af ofrene herfor, og om*

erstatning af Rådets rammeafgørelse 2002/629/RIA. Hentede 28. maj 2015 fra eur-lex.europa.eu: eur-lex.europa.eu/legal-content/DA/TXT/?uri=CELEX:32011L0036

European Commission. (25. januar 2012). *ec.europa.eu, Commission Proposal for a Regulation of the European Parliament and of the Council, art. 4(2), COM (2012) 11 final (Jan. 25, 2012).* Hentede 16. april 2015 fra ec.europa.eu: ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf

European Commission. (2014a). *Ethics and Security of Surveillance Technologies.* European Commission, European Group on Ethics in Science and New Technologies to the European Commision. Brussels: European Commission.

European Commission. (2013). *Options for Strengthening Responsible Research and Innovation.* Europa Commission. Brussels: European Commission.

European Commission. (2014b). *Progress on EU data protection reform now irreversible following European Parliament vote.* European Commission. Starsbourg: European Commission.

European Commission. (2014c). *Towards a thriving data-driven economy.* European Commission. Brussels: European Commission.

European Union Agency for Fundamental Rights. (2013). *Handbook on European data protection law.* Belgien: Council of Europe.

Europæiske Union. (6. maj 2010). *europa.eu, Resumeer af EU-lovgivningen: Chartret om grundlæggende rettigheder*. Hentede 31. marts 2014 fra europa.eun: europa.eu/legislation_summaries/justice_freedom_security/combating_discrimination/l33501_da.htm

EUROPOL. (2011). *EU Organised crime threat assessment.* EUROPOL, European Police Office.

EUROPOL. (2014). *The Internet Organised Crime Threat Assessment (iOCTA).* EUROPOL. The Haque: European Police Office.

Executive Office of the President. (2014). *BIG DATA: SEIZING OPPORTUNITIES, PRESERVING VALUES.* The White House, Executive Office of the President. Washington: The White House.

Export.gov. (30. 1 2009). *export.gov, Safe Harbor Enforcement Overview.* Hentede 3. november 2014 fra export.gov: export.gov/safeharbor/eu/eg_main_018481.asp

Facebook. (30. januar 2015a). *facebook.com, Datapolitik*. Hentede 5. maj 2015 fra facebook.com: facebook.com/about/privacy

Facebook. (30. januar 2015b). *facebook.com, Erklæring om rettigheder og ansvar*. Hentede 5. maj 2015 fra facebook.com: facebook.com/legal/terms

Ferrara, E., De Meo, P., & Catanese, S. (juli 2014). Visualizing criminal networks reconstructed from mobile phone records. *Social and Information Network* .

Flanagan, M., Howe, D. C., & Nissenbaum, H. (2008). Embodying Values in Technology: Theory and Practice. I J. Van Den Hoven, & J. Weckert, *Information Technology and Moral Philosophy* (s. 322-352). Cambridge: Cambridge University Press.

Flanagan, M., Howe, D. C., & Nissenbaum, H. (April 2005). Values at Play: Design Tradeoffs in Socially-Oriented Game Design. *Proceedings of the SIGCHI Conference on human factors in computing systems* , s. 751-760.

Floridi, L. (November 2012). Big Data and Their Epistemological Challenge. (L. Floridi, Red.) *Philosophy & Technology , 25* (4), s. 435-437.

Floridi, L. (december 2005). The ontological interpretation of informational privacy. *Ethics and Information Technology , 7* (4), s. 185-200.

Folketingets EU-oplysning. (u.d.). *eu-oplysningen.dk, Konvention til Beskyttelse af Menneskerettigheder og Grundlæggende Frihedsrettigheder (1950)*. Hentede

31. marts 2014 fra eu-oplysningen.dk: eu-oplysningen.dk/dokumenter/konventioner/echr/

Foucault, M. (1995). *Discipline and Punish: The Birth of the Prison* (2. udgave udg.). (A. Sheridan, Ovs.) New York, USA: Vintage Books.

Foucault, M. (2002). *Overvågning og straf.* (M. C. Jacobsen, Ovs.) Frederiksberg, Danmark: DET lille FORLAG.

Fried, C. (1984). Privacy [a moral analysis]. I F. D. Schoeman (Red.), *Philosophical Dimensions of Privacy: An Anthology* (s. 203-222). Cambridge University Press.

Friedman, B., & Kahn, P. H. (2003). Human values, ethics, and design. I J. A. Jacko, & A. Sears, *The human-computer interaction handbook.* Hillsdale, USA: L. Erlbaum Assoc. Inc.

Friedman, B., Hook, K., Gill, B., Eidmar, L., Prien, C. S., & Severson, R. (18-22. august 2008). Personlig Integritet: A Comparative Study of Perceptions of Privacy in Public Places in Sweden and the United States. *2008 NordiCHI* .

Friedman, B., Kahn, P. H., & Borning, A. (2006). Value Sensitive Design and Information Systems. I P. Zhang, & D. Galletta (Red.), *Human-Computer Interaction and Management Information Systems: Foundations* (s. 348-372). Armonk, New York, USA: M.E. Sharpe.

Friedman, B., Kahn, P. H., & Borning, A. (2. december 2001). Value Sensitive Design: Theory and Methods. *UW CSE Technical Report* .

Friedman, B., Lin, P., & Miller, J. K. (2005). Informed Consent by Design. I L. F. Cranor, & S. Garfinkel (Red.), *Security and Usability* (s. 503-529). O'Reilly Media.

Gandy, O. H. (1996). Coming to Terms with the Panoptic Sort. I D. Lyon, & E. Zureik (Red.), *Computers, Surveillance, and Privacy* (s. 132-155). Minneapolis, USA: University of Minnesota Press.

Gavison, R. (1984). Privacy and the limits of law. I F. D. Schoeman (Red.), *Philosophical Dimensions of Privacy: An Anthology* (s. 346-402). Cambridge University Press.

Gürses, F. S. (maj 2010). *Multilateral Privacy Requirements Analysis in Online Social Network Services* . Katholieke Universiteit Leuven, Faculty of Engineering, Department og Computer Science.

Gürses, F. S., Troncoso, C., & Diaz, C. (2011). Engineering Privacy by Design. *Computers, Privacy & Data Protection* .

Generalsekretariatet for Rådet og Kommisionen. (7. februar 1992). *europa.eu, Traktat som Den Europæiske Union.* Hentede 2. august 2015 fra europa.eu: europa.eu/eu-law/decision-making/treaties/pdf/treaty_on_european_union/treaty_on_european_union_da.pdf

Gerber, M. S. (maj 2014). Predicting crime using Twitter and kernel density estimation. *Decision Support Systems , 61*, s. 115-125.

Gerstein, R. S. (1984a). Intimacy and privacy. I F. D. Schoeman (Red.), *Philosophical Dimensions of Privacy: An Anthology* (s. 265-271). Cambridge University Press.

Gerstein, R. S. (1984b). Privacy and self-incrimination. I F. D. Schoeman (Red.), *Philosophical Dimensions of Privacy: An Anthology* (s. 245-264). Cambridge University Press.

Giannotti, F., Monreale, A., & Pedreschi, D. (2013). Mobility Data and Privacy. I C. Renso, S. Spaccapietra, & E. Zimányi (Red.), *Mobility Data: Modeling, Management, and Understanding* (s. 174-194). Cambridge University Press.

Greenwald, G. (2014). *No place to hide: Edward Snowden, the NSA and the surveillance state* (1. udg.). London, England: Hamish Hamilton, Pinguin Books.

Greenwald, G. (6. juni, 2013). *The Guardian, NSA collecting phone records of millions of Verizon customers daily*. Hentede 10. maj 2015 fra The Guardian:

theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order

Greenwald, G. (31. juli, 2013). *The Guardian, XKeyscore: NSA tool collects 'nearly everything a user does on the internet'*. Hentede 10. maj 2015 fra The Guardian: theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data

Hastrup, T. (1976). *Latin-dansk ordbog* (5. udg.). København, Denmark: Gyldendal.

Heede, D. (2010). *Det tomme menneske. En introduktion til Foucault.* (2. udg.). København S, Danmark: Museum Tusculanum.

Hilbert, M. (jan 2013). *Big Data for Development: From Information- to Knowledge Societies.* Hentede 18. maj 2015 fra papers.ssrn.com: ssrn.com/abstract=2205145

Hiranandani, V. (oktober 2011). Privacy and security in the digital age: contemporary challenges and future directions. *The International Journal of Human Rights , 15* (7), s. 1091-1106.

Hobbes, T. (2001). *Leviathan.* South Bend, IN, USA: Informotions, Inc.

Hobbes, T. (2008). *Leviathan* (1. udg.). (C. B. Østergaard, Ovs.) København, Danmark: Informations Forlag.

Hogan, J. (2003. juli 2003). *newscientist.com, Smart software linked to CCTV can spot dubious behaviour*. Hentede 15. juli 2014 fra newscientist.com: newscientist.com/article/dn3918-smart-software-linked-to-cctv-can-spot-dubious-behaviour.html#.U8SCmFbmRWE

Houses of Parliament. Parliamentary Office of Science & Technology. (juli 2014). *researchbriefings.parliament.uk, Big Data: An Overview.* Hentede 17. august 2015 fra researchbriefings.parliament.uk: researchbriefings.parliament.uk/ResearchBriefing/Summary/POST-PN-468/#fullreport

Hu, X., & Liu, H. (2012). Text Analytics in Social Media. I *Mining Text Data* (s. 385-414). Springer US.

Human Rights Council, United Nations. (2014). *The Right to Privacy in the Digital Age, Report of the Office of the United Nations High Commissioner for Human Rights,.* United Nations.

Hume, D. (1999). *A TREATISE OF Human Nature: BEING An ATTEMPT to introduce the experimental Method of Reasoning INTO MORAL SUBJECTS.* Kitchener, Ontario, Canada: Batoche Books.

Hypponen, M. (Oktober 2013). *ted.com, How the NSA betrayed the world's trust - time to act*. Hentede 11. maj 2015 fra ted.com: ted.com/talks/mikko_hypponen_how_the_nsa_betrayed_the_world_s_trust_time_to_act/transcript?language=en#t-30705

Institut for Menneskerettigheder. (2013). *Databeskyttelse Status 2013.* Institut for Menneskerettigheder.

Institut for Menneskerettigheder. (2015). *Databeskyttelse, status 2014-15.* Institut for Menneskerettigheder, København.

Jarlov, R. (25. februar 2015). *politiken.dk, Hvorfor skal vi overvåges, hvis vi ikke har noget at skjule?* Hentede 2. august 2015 fra politiken.dk: politiken.dk/debat/profiler/rasmus-jarlov/ECE2562671/hvorfor-skal-vi-overvaages-hvis-vi-ikke-har-noget-at-skjule/

Jespersen, J. L., Albrechtslund, A., Øhrstrøm, P., Hasle, P., & Albertsen, J. (2007). Surveillance, Persuasion, and Panopticon. *Persuasive Technology , 4744*, s. 109-120.

Joh, E. E. (marts 2014). Policing by numbers: big data and the Fourth Amendment. *Washington Law Review , 89* (1), s. 35-68.

Johnson, E. H. (februar 2000). Getting Beyond the Simple Assumptions of Organizational Impact . *Bullentin og the American Society for Information Science , 26* (3), s. 18-19.

Judgement of the court (Grand Chamber). (24. april 2014). *In Joined Cases C-293/12 and C-594/12*. Hentede 16. august 2015 fra curia.europa.eu: curia.europa.eu/juris/document/document.jsf?text=&docid=150642&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=65035

Justitsministeriet. (u.d.). *justitsministeriet.dk, Terrorbekæmpelse*. Hentede 15. august 2015 fra justitsministeriet.dk: justitsministeriet.dk/arbejdsområder/politi-og-straf/terrorbekæmpelse

Justitsministeriet. (2. juni, 2014). *Notat om betydningen af EU-Domstolens dom af 8. april 2014 i de forenede sager C-293/12 og C-594/12 (om logningsdirektivet) for de danske logningsregler.* Justitsministeriet, Lovafdelingen, EU-retskontoret. Justitsministeriet.

Justitsministeriet. (24. august 2015). *Notat til Folketingets Europaudvalg og Folketingets Retsudvalg om afgivelse af indlæg i EU-Domstolens sag C-203/15, Tele2 Sverige AB mod Post- og telestyrelsen.* Hentede 26. september 2015 fra ft.dk: ft.dk/samling/20142/almdel/reu/bilag/48/1541864.pdf

Kant, I. (2002). *Groundwork for the Metaphysics of Morals.* (A. W. Wood, Ovs.) New Haven, Connecticut, USA: Yale University Press.

Kant, I. (1781). *Grundlegung zur Metaphysik der Sitten.* (T. Bøgeskov, Ovs.) Hentede 19. marts 2015 fra korpora.org: korpora.org/Kant/aa04/Inhalt4.html

Kant, I. (1785). *Grundlegung zur Metaphysik der Sitten.* (T. Bøgeskov, Ovs.) Hentede 19. marts 2015 fra korpora.org: korpora.org/Kant/aa04/Inhalt4.html

Keim, D., Qu, H., & Ma, K.-L. (2013). Big-Data Visualization. *IEEE Computer Craphics and Application , 33* (4), s. 50-51.

Kjølbro, J. F. (2005). *Den Europæiske Menneskerettdighedskonvention - for praktikere* (1. udgave udg.). Jurist og økonomforbundet.

Klitou, D. (2014). The Value, Role and Challenges of Privacy by Design. I K. Demetrius (Red.), *Privacy-Invading Technologies and Privacy by Design. Safeguarding Privacy, Liberty and Security in the 21st Century* (s. 259-288). T.M.C. Asser Press.

Kosinski, M., Stillwell, D., & Greapel, T. (2013). Private traits and attributes are predictable from digital records of human behavior. (K. Wachter, Red.) *Proceedings of the National Academy of Sciences , 110* (15), s. 5802-5805.

Kupfer, J. (1987). Privacy, autonomy, and self-concept. *American Philosophical Quarterly , 24* (1), s. 81-89.

Laney, D. (6. februar 2001). *blogs.gartner.com, 3D Data Management: Controlling Data Volume, Velocity, and Variety.* Hentede 8. august 2014 fra blogs.gartner.com: blogs.gartner.com/doug-laney/files/2012/01/ad949-3D-Data-Management-Controlling-Data-Volume-Velocity-and-Variety.pdf

Lauritsen, P. (2011). *Big Brother 2.0. Danmark som overvågningssamfund* (1. udg.). København K, Danmark: Informations forlag.

Le Dantec, C. A., Poole, E. S., & Wyche, S. P. (april 2009). Values as Lived Experince: Evolving Value Sensitive Design in Support of Value Discovery. *Proceedings of the SIGCHI Conference on human factors in computing system* , s. 1141-1150.

Lerman, J. (3. September 2013). Big Data and Its Exclusions. *Stanford Law Review Online , 66*, s. 55-63.

Liotta, P. H. (december 2002). Boomerang Effect: The Convergence of National and Human Security. *Security Dialogue , 33* (4), s. 473-488.

Locke, J. (2003). *Two Treatises of Government and a Letter Concerning Toleration.* (I. Shapiro, Red.) New Haven, Connecticut, USA: Yale University Press.

Lovbekendtgørelse nr. 1148 af 9. december 2011. (u.d.). Lovbekendtgørelse nr. 1148 af 9. december 2011 om krav til information og samtykke ved lagring af eller adgang til oplysninger i slutbrugeres terminaludstyr.

Lovbekendtgørelse nr. 59, af 16. maj 1991. (u.d.). Lovbekendtgørelse nr. 59, af 16. maj 1991 om beskyttelse af det enkelte menneske i forbindelse med elektronisk databehandling af personoplysninger.

Lovbekendtgørelse nr. 660 af 19. juni 2014. (u.d.). Lovbekendtgørelse nr. 660 af 19. juni 2014 om ændring af bekendtgørelse om udbydere af elektroniske kommunikationsnets og elektroniske kommunikationstjenesters registrering og opbevaring af oplysninger om teletrafik (logningsbekendtgørelsen).

Lovbekendtgørelse nr. 988 af 28. september 2006. (u.d.). Lovbekendtgørelse nr. 988 af 28. september 2006 om udbydere af elektroniske kommunikationsnets og elektroniske kommunikationstjenesters registrering og opbevaring af oplysninger om teletrafik (logningsbekendtgørelsen).

Lund, A. A. (2007). *Dansk-Latin Ordbog* (1. udgave udg.). Copenhagen, Denmark: Gyldendal.

Lyon, D. (2003). Surveillance as social sorting. Computer codes and mobile bodies. I D. Lyon (Red.), *Surveillance as Social Sorting: Privacy, Risk, and Digital Discrimination* (s. 13-30). New York, New York, USA: Routlegde.

Lyon, D. (2007). *Surveillance studies: an overview* (1. udg.). Cambrigde, UK: Polity Press.

Lyon, D. (2003). Surveillance Technology and Surveillance Society. I T. J. Misa, P. Brey, & A. Feenberg (Red.), *Modernity and technology* (s. 161-184). Massachusetts, USA: MIT.

Lyon, D. (2014). The Emerging Surveillance Culture. I A. Jansson, & M. Christensen (Red.), *Media, surveillance and identity: social perspectives* (1. udg.). New York, New York, USA: Peter Lang Publishing.

MacAskill, E., Borger, J., Nick, H., Davies, N., & Ball, J. (21. juni 2013). *theguardian.com, GCHQ taps fibre-optic cables for secret access to world's communications*. Hentede 1. maj 2015 fra theguardian.com: theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa

Manders-Huits, N. (12. marts 2011). What Values in Design? The Challenge of Incorporating Moral Values into Design. *Science and Engineering Ethics , 17* (2), s. 271-287.

Mann, S., Nolan, J., & Wellman, B. (2003). Sousveillance: Inventing and Using Wearable Computing Devices for Data Collection in Surveillance Environments. *Surveillance and Society , 1* (3), s. 331-355.

Marwick, A. E. (2012). The Public Domain: Social Surveillance in Everyday Life. *Surveillance and Society , 9* (4), s. 378-393.

Marx, G. (2002). What's New About the "New Surveillance"? Classifying for Change and Continuity. *Surveillance and Society , 1* (1), s. 9-29.

Mayer-Schönberger, V., & Cukier, K. (2013). *Big data: a revolution that will transform how we live, work and think.* USA: John Murray.

McKinsey Global Institute. (2011). *Big data: The next frontier for innovation, competition and productivity.* McKinsey & Company. McKinsey Institute.

Monreale, A. (21. june 2011). Privacy by Design in Data Mining. Pisa, Italia: Department og Computer Science, University of Pisa.

Moor, J. H. (september 1997). Towards a Theory of Privacy in the Information Age. *ACM SIGCAS Computers and Society , 27* (3), s. 27-32.

Moor, J. H. (oktober 1985). What is Computer Ethics? *Metaphilosophy , 16* (4), s. 266-275.

Moor, J. (marts 1998). Reason, Relativity, and Responsibility in Computer Ethics. *ACM SIGCAS Computers and Society , 28* (1), s. 14-21.

Nissenbaum, H. (2001, marts). How computer systems embody values. *Computer , 34, 45* (3), pp. 120, 118-119.

Nissenbaum, H. (2004). Privacy as contextual integrity. *Washington Law Review* (79), pp. 119-158.

Nissenbaum, H. (2010). *Privacy in context: technology, policy, and the integrity of social life.* Stanford Law Books.

Nissenbaum, H., & Gaboury, J. (21. september 2012). *nyu.edu, Values In Design*. Hentede 16. august 2015 fra nyu.edu: nyu.edu/projects/nissenbaum/vid/about.html

Obama, B. (u.d.). *whitehouse.gov, Memorandum for the Heads of Executive Departments and Agencies*. Hentede 13. maj 2014 fra whitehouse.gov: whitehouse.gov/the_press_office/TransparencyandOpenGovernment

OECD. (2013). *The OECD Privacy Framework.* Hentet fra http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf

Oosterlaken, I. (april 2015). Applying Value Sensitive Design (VSD) to Wind Turbines and Wind Parks: An Exploration. *Science and Engineering Ethics , 21* (2), s. 359-379.

ordbogen.com, examination. (u.d.). Hentede 20. marts 2015 fra rdbogen.com, examination: ordbogen.com/opslag.php?word=examination&dict=auto&wcl=3&wci=3fd8cd16-fe44-469d-b231-5ee28768f3ee

ordbogen.com, sikkerhed. (u.d.). Hentede 22. december 2014 fra ordbogen.com: ordbogen.com/opslag.php?word=sikkerhed&dict=auto

ordbogen.com, sur. (u.d.). Hentede 17. februar 2015 fra ordbogen.com: ordbogen.com/opslag.php?word=sur&dict=a002

ordbogen.com, veiller. (u.d.). Hentede 17. februar 2015 fra ordbogen.com: ordbogen.com/opslag.php?word=veiller&dict=a002

ordnet.dk, diskrimination. (u.d.). (Det Danske Sprog- og Litteraturselskab) Hentede 12. februar 2015 fra ordnet.dk: ordnet.dk/ddo/ordbog?query=diskrimination

ordnet.dk, overvåge. (u.d.). (Det Danske Sprog- og Litteraturselskab) Hentede 11. september 2014 fra ordnet.dk: http://ordnet.dk/ddo/ordbog?query=overvåge&search=Søg

ordnet.dk, privat. (u.d.). (Det Danske Sprog- og Litteraturselskab) Hentede 12. februar 2015 fra ordnet.dk: ordnet.dk/ddo/ordbog?query=privat

ordnet.dk, Privatliv. (u.d.). (Det Danske Sprog- og Litteraturselskab) Hentede 26. Februar 2015 fra ordnet.dk: http://ordnet.dk/ddo/ordbog?query=privatliv&search=Søg

ordnet.dk, sikker. (u.d.). Hentede 11. februar 2015 fra ordnet.dk: ordnet.dk/ddo/ordbog?query=sikker

Orwell, G. (1949). *1984* (9. udg.). (P. Monrad, Ovs.) Gyldendal.

Owen, T. (juni 2004). Challenges and opportunities for defining and measuring human security. *Disarmament Forum* (2).

oxforddictionaries.com, privacy. (u.d.). Hentede 26. Februar 2015 fra oxforddictionaries.com: oxforddictionaries.com/definition/english/privacy?searchDictCode=all

oxforddictionaries.com, safety. (u.d.). Hentede 22. december 2014 fra oxforddictionaries.com: oxforddictionaries.com/definition/english/safety?searchDictCode=all

oxforddictionaries.com, security. (u.d.). Hentede 22. december 2014 fra oxforddictionaries.com,: oxforddictionaries.com/definition/english/security?searchDictCode=all

Paris, R. (oktober 2001). Human Security: Paradigm Shift or Hot Air? *International Security , 26* (2), s. 87-102.

Pearson, J. (26. april 2014). *motherboard.vice.com, Twitter Can Now Predict Crime, And That Raises Serious Questions*. Hentede 9. juli 2014 fra motherboard.vice.com: motherboard.vice.com/blog/twitter-can-predict-crime-raising-serious-and-urgent-questions

Peissl, W. (marts 2003). Surveillance and Security: A Dodgy Relationship. *Journal of Contingencies and Crisis Management , 11* (1), s. 19-24.

Perry, W. L., McInnis, B., Price, C. C., Smith, S. C., & Hollywood, J. S. (2013). *Predictive Policing. The Role of Crime Forecasting in Law Enforcement Operations.* RAND Corporation, Safety and Justice Program. RAND Corporation.

Petersen, R. R., & Wiil, U. K. (december 2013). CrimeFighter Investigator: Integrating synthesis and sense-making for criminal network investigation. *Security Informatics , 2* (1), s. 1-13.

Ploug, T. (2003). Privathed og overvågning af e-mails. I P. Øhrstrøm (Red.), *IT-etiske temaer* (s. 65-87). Kolding, Danmark: Institut for Fagsprog, Kommunikation og Informationsvidenskab, Syddansk Universitet.

Polanyi, M. (1983). *The tacit dimension.* Gloucester, Massachuetts, USA: Peter Smith.

Polonetsky, J., & Tene, O. (3. september 2013). Privacy and Big Data: Making Ends Meet. *Stanford Law Review Online , 66*.

Posner, R. A. (1984). An economic theory of privacy. I F. D. Schoeman (Red.), *Philosophical dimensions of Privacy: An Anthology* (s. 333-345). Cambridge University Press.

PRISE. (2007). *D 2.2 Overview of Security Technologies v 1.1.*

PRISE. (u.d.). PRISE Concluding Conference Statement Paper.

Proportionalitetsprincippet. (u.d.). Hentede marts. 31 2014 fra Europa Resumeer af EU-lovgivningen: http://europa.eu/legislation_summaries/glossary/proportionality_da.htm

Rachels, J. (1984). Why privacy is important. I F. D. Schoeman (Red.), *Philosophical Dimensions of Privacy: An Anthology* (s. 290-299). Cambridge University Press.

Rachels, J., & Rachels, S. (2010). *The Elements of Moral Philosphy* (6. udg.). McGraw-Hill.

Raguse, M. (2008). *Deliverable 3.2 Legal Evaluation Report.* PRISE.

Raguse, M., Meints, M., Langfeldt, O., & Peissl, W. (2008). *Deliverable 6.2 - Criteria for privacy enhancing security technologies.*

Ratcliffe, J. H. (2003). Intelligence-led Policing. *Trends and Issues in Crime and Criminal Justice* (248), s. 1-5.

Ratcliffe, J. H. (2011). *Intelligence-Led Policing.* New York, USA: Routledge.

Rønn, K. V. (2013). Democratizing Strategic Intelligence?: On the feasibility of an objective, decision-making framework when assessing threats and harms of organized crime. *Policing , 7* (1), s. 53-62.

Regan, P. M. (1995). *Legislating Privacy: Technology, Social Values, and Public Policy .* USA: The University of North Carolina Press.

Regan, P. M. (8. december 2002). Privacy as a Common Good in the Digital World. *Information, Communication & Society , 5* (3), s. 382-405.

Regan, P. M. (2011). Response to Bennet: Also in defence of privacy. *Surveillance and Society , 8* (4), s. 497-499.

Regeringen. (2015). *Et stærkt værn mod terror. 12 nye tiltag mod terror.* København: Regeringen.

Reiman, J. H. (1995). Driving to the Panopticon: A Philosophical Exporation of the Risks to Privacy Posed by the Highway Technology of the Future. *Santa Clara High Technology Law Journal , 11* (1), s. 27-44.

Reiman, J. H. (1984). Privacy, intimacy, and personhood. I F. D. Schoeman (Red.), *Philosophical Dimensions of Privacy: An Anthology* (s. 300-316). Cambridge University Press.

Richards, N. M. (2013). The Dangers of Surveillance. *Harward Law Review , 126* (7).

Richards, N. M., & King, J. H. (3. september 2013). Three Paradoxes of Big Data. *Stanford Law Review Online , 66*, s. 41-46.

Rosen, J. (13. februar 2012). The Right to Be Forgotten. *Stanford Law Review Online , 64*, s. 88-92.

Rule, J. B. (1973). *Private Lives and Public Surveillance.* London, Great Britian: Allen Lane.

Schaefer, A., Bahney, B., & Riley, K. J. (2009). *Security in Mexico Implications for U.S. Policy Options.* Rand Corporation.

Schneier, B. (27. februar 2014). *theguardian.com, NSA robots are 'collecting' your data, too, and they're getting away with it*. Hentede 5. maj 2015 fra theguardian.com: theguardian.com/commentisfree/2014/feb/27/nsa-robots-algorithm-surveillance-bruce-schneier

Schoeman, F. D. (1984). Privacy and intimate information. I F. D. Schoeman (Red.), *Philosophical Dimensions of Privacy: An Anthology* (s. 403-418). Cambridge University Press.

Schremer, B. W., Custers, B., & van der Hof, S. (june 2014). The crisis of consent: how stronger legal protection may lead to weaker consent in data protection. *Ethics and Information Technology , 12* (2), s. 171-182.

Secretary's Advisory Committee on Automated Personal Data Systems . (1973). *Records, Computers and the Rights of Citizens.* U.S Deparment of of Health, Education and Welfare.

Sicular, S. (27. marts 2013). *forbes.com, Gartner's Big Data Definition Consists of Three Parts, Not to Be Confused with Three "V"s*. Hentede 8. august 2014 fra

forbes.com: forbes.com/sites/gartnergroup/2013/03/27/gartners-big-data-definition-consists-of-three-parts-not-to-be-confused-with-three-vs/

Siewert, S. B. (9. juli 2013). *ibm.com, Big data in the cloud. Data velocity, volume, variety, veracity*. (IBM) Hentede 8. august 2014 fra ibm.com: ibm.com/developerworks/library/bd-bigdatacloud/index.html?ca=dat

Silke, A. (2008). Research on terrorism. A Review of the Impact of 9/11 and the Global War on Terrorism. I H. Chen, E. Reid, J. Sinai, A. Silke, & B. Ganor (Red.), *Terrorism Informatics. Knowledge Management and Data Mining for Homeland Security* (Årg. 18, s. 27-49). Springer US.

Smith, E. (1. januar 2010). *Politiken.dk, Vil vore børnebørn vokse op som frie?* Hentede 11. september 2014 fra Politiken.dk: politiken.dk/debat/kroniken/ECE869776/vil-vore-boerneboern-vokse-op-som-frie/

Solove, D. (september 2007). 'I've Got Nothing to Hide' and Other Misunderstandings of Privacy. *San Diego Law Review , 44* (4), s. 745-772.

Solove, D. (13. October 2012). *linkedin.com, On Privacy, Why Is the EU So Different from the US?* Hentede 21. juli 2014 fra linkedin.com: linkedin.com/today/post/article/20121023040724-2259773-on-privacy-why-is-the-eu-so-different-from-the-us

Stalder, F. (2002). Opinion. Privacy is not the antidote to surveillance. *Surveillance and Society , 1* (1), s. 124-124.

Stalder, F., & Lyon, D. (2003). Electronic identity cards and social classification. I D. Lyon (Red.), *Surveillance as Social Sorting: Privacy, Risk, and Digital Discrimination* (s. 77-93). New York, New York, USA: Routlegde.

Stowers, G. (2013). *The Use of Data Visualization in Government.* San Francisco State Univerity, School of Public Affairs and Civic Engagement. IBM Center for The Business of Government.

Sweeney, L. (oktober 2002). k-ANONYMITY: A MODEL FOR PROTECTING PRIVACY. *International Journal on Uncertainty, Fuzziness and Knowlegde-based Systems , 10* (5), s. 557-570.

Tavani, H. T. (june 1999). Informationel privacy, data mining, and the Internet. *Ethics and Information Technology , 1* (2), s. 137-145.

The City of New York. (8. august 2012). *nyc.gov, The City of New York, NEWS from the BLUE ROOM*. Hentede 21. maj 2015 fra nyc.gov: nyc.gov/portal/site/nycgov/menuitem.c0935b9a57bb4ef3daf2f1c701c789a0/index.jsp?pageID=mayor_press_release&catID=1194&doc_name=http://www.nyc.gov/html/om/html/2012b/pr291-12.html&cc=unused1978&rc=1194&ndi=1

The European Union. (15. september 2004). *consilium.europa.eu, A Human Security Doctrine for Europe. The Barcelona Report on the Study of the Group on Europ's Security Capabilities*. Hentede 16. august 2015 fra consilium.europa.eu: consilium.europa.eu/uedocs/cms_data/docs/pressdata/solana/040915capbar.pdf

The Times Editorial Board. (12. august 2014). *latimes.com, The 'terrorist screening database': Are they all terrorists?* Hentede 15. august 2014 fra latimes.com: latimes.com/opinion/editorials/la-ed-terrorist-screening-database-20140813-story.html

Thomson, J. J. (1984). The Right to Privacy. I F. D. Schoeman (Red.), *Philosophical Dimensions of Privacy: An Anthology* (s. 272-289). Cambridge University Press.

Thuraisingham, B. (december 2002). Data Mining, National Security, Privacy and Civil Liberties. *ACM SIGKDD Explorations Newsletter , 4* (2), s. 1-5.

Timmermans, J., & Mittelstadt, B. (2014). Reflexivity and Value-sensitive design. *CEPE 2014 Proceeding.* Paris.

Timmermans, J., Zhao, Y., & van den Hoven, J. (december 2011). Ethics and Nanopharmacy: Value Sensitive Design of New Drugs. *Nanoethics , 5* (3), s. 269-283.

U.S. Department of Commerce. (u.d.). *export.gov, U.S.-EU Safe Harbor Overview*. Hentet fra export.gov: export.gov/safeharbor/eu/eg_main_018476.asp

United Nations Development Programme. (1994). New dimensions of human security. I *Human Development Report* (s. 1-226). Oxford University Press.

United States Courts. (u.d.). *uscourts.gov, Fourth Amendment*. Hentede 23. marts 2015 fra uscourts.gov: uscourts.gov/educational-resources/get-involved/constitution-activities/fourth-amendment.aspx

United States Government Accountability Office. (2013). *Information resellers. Consumer Privacy Framework Needs to Reflect Changes in Technology and the Marketplace.* Report to the Chairman, Committee on Commerce, Science, and Transportation, U.S. Senate.

ValuesAtPlay.org. (2005). *valuesAtPlay.org*. Hentede 2. juni 2015 fra valuesatplay.org

van den Hoven, J. (2007). ICT and Value Sensitive Design. *The Information Society: Innovation, Legitimacy, Ethics and Democracy In honor of Professor Jacques Berleur s.j , 233*, pp. 67-72.

van den Hoven, J. (September 1997). Privacy and the Varieties of Moral Wrong-doing in an Information Age. *ACM SIGCAS Computers and Society* (3), s. 33-37.

van den Hoven, J. (1999). Privacy or Informational Injustice. I L. J. Pourciau (Red.), *Ethics and Electronic Information in the Twenty-First Century* (s. 130-150).

van den Hoven, J. (2013). Value Sensitive Design and Responsible Innovation. I R. Owen, J. Bessant, & M. Heintz (Red.), *Responsible innovation: managing the*

responsible emergence of science and innovation in society (1. udg., s. 75-83). John Wiley and Sons, Ltd.

van den Hoven, J., & Manders-Huits, N. (2012). Value-sensitive Design. I J. K. Friis, S. A. Pedersen, & V. F. Hendricks (Red.), *A Companion to the Philosophy of Technology* (s. 477-480). Wiley-Blackwell.

van den Hoven, J., Lokhorst, G.-J., & Poel, I. V. (1. marts 2011). Engineering and the Problem of Moral Overload. *Science and Engineering Ethics , 18* (1), s. 143-155.

van Kempen, P. H. (2013). Four Concepts of Security - A Human Rights Perspective. *Human Rights Law Review , 13* (1), s. 1-23.

van Lieshout, M., Friedewald, M., Wright, D., & Gutwirth, S. (2013). Reconciling privacy and security. *Innovation , 26* (1-2), s. 119-132.

van Loenen, B., Groetelaers, D., Zevenbergen, J., & de Jong, J. (2007). Privacy versus national security: The impact of privacy law on the use of location technology for national security purposes. *The European Information Society* , s. 135-152.

Vedder, A. (2011). Privacy 3.0. I S. van der Hof, & M. M. Groothuis (Red.), *Innovating Government. Normative, Policy and Technological Dimensions of Modern Government* (s. 17-28). T.M.C. Asser Press.

Verbeek, P.-P. (2005). *What Things Do. Philosophical reflections on technology, agency, and design.* (R. P. Crease, Ovs.) Pennsylvania, USA: Pennsylvania State University Press.

Verfaillie, K., Beken, T. V., & Defruytier, M. (2006). Thinking about the future and long-term assessments. A methodological study. I T. V. Beken (Red.), *European Organised Crime Scenarios for 2015* (s. 9-35). Maklu Publishers.

Walzer, M. (1995). *Spheres of justice: a defense of pluralism and equality.* Blackwell Publishers.

Wang, Y., & Kobsa, A. (2008). Privacy-Enhancing Technologies. I M. Gupta, & R. Sharman, *Handbook of Research on Social and Organizational Liabillities in Information Security* (s. 203-227).

Warnier, M., Dechesne, F., & Brazier, F. (2015). Design for the Value of Privacy. I J. van den Hoven, P. E. Vermaas, & I. van de Poel (Red.), *Handbook of Ethics, Values, and Technological Design. Sources, Theory, Values and Application Domains* (1 udg., s. 431-445). Springer Netherlands.

Warren, S. D., & Brandeis, L. D. (1984). The Right to Privacy (The implicit made explicit). I F. D. Schoeman (Red.), *Philosophical Dimensions of Privacy: An Anthology* (s. 75-103). Cambridge University Press.

Wasserstrom, R. A. (1984). Privacy: some arguments and assumptions. I F. D. Schoeman (Red.), *Philosophical Dimensions of Privacy* (s. 317-332). Cambridge University Press.

Weisburd, D., & McEvan, T. (1997). Introduction: Crime Mapping and Crime Prevention. I D. Weisburd, & T. McEvan, *Crime Mapping and Crime Prevention Studies.* Monsey, New York, USA.

Westin, A. (1984). The origins of modern claims to privacy. I F. D. Schoeman (Red.), *Philosophical Dimensions of Privacy: An Anthology* (s. 56-74). Cambridge University Press.

Wiil, U. K., Gniadek, J., Memon, N., & Petersen, R. R. (2013). Knowledge Management Tools for Terrorist Network Analysis. I *Knowledge Discovery, Knowledge Engineering and Knowledge Management. Second International Joint Conference, IC3K 2010, Valencia, Spain, October 25-28, 2010, Revised Selected Papers.* (s. 322-337). Springer Berlin Heidelberg.

Wiil, U. K., Memon, N., & Gniadek, J. (2011). CrimeFighter: A Toolbox for Counterterrorism. I A. Freds, J. L. Dietz, K. Liu, & J. Filipe (Red.), *Knowledge Discovery, Knowledge Engineering and Knowledge Management. First International Joint Conference, IC3K 2009, Funchal, Madeira, Portugal, October 6-8, 2009, Revised Selected Papers* (s. 337-350). Springer Berlin Heidelberg.

Wikipedia, algorithmic trading. (u.d.). *en.wikipedia.org, algorithmic trading*. Hentede 6. november 2014 fra en.wikipedia.org: en.wikipedia.org/wiki/Algorithmic_trading

Wikipedia, AOL search data leak. (u.d.). *en.wikipedia.org, AOL search data leak*. Hentede 3. november 2015 fra en.wikipedia.org: en.wikipedia.org/wiki/AOL_search_data_leak

Wikipedia, big data. (u.d.). *en.wikipedia.org, big data*. Hentede 20. maj 2015 fra en.wikipedia.org: en.wikipedia.org/wiki/Big_data

Wood, D. M., & Webster, W. R. (2011). The Normality of Living in Surveillance Societies. I M. M. Groothuis, & S. van der Hof (Red.), *Innovating Government. Normative, Policy and Technological Dimensions of Modern Government* (s. 151-164). T.M.C. Asser Press.

Wulff, H. R., Pedersen, S. A., & Rosenberg, R. (1999). *Medicinsk filosofi* (1 udg.). Broadview Press.

Xu, H., Crossler, R. E., & Bélanger, F. (december 2012). A Value Sensitive Design Investigation of Privacy Enhancing Tools in Web Browsers. *Decision Support Systems , 54* (1), s. 424-433.

Xu, J., & Chen, H. (juni 2005). Criminal network analysis and visualization. *Communications of the ACM , 48* (6), s. 101-107.

Øhrstøm, P. (2003). Anvendt etik - argumentation og samfundsdebat. I P. Øhrstrøm (Red.), *IT-etiske temaer* (1 udg., s. 21-41). Kolding, Danmark: Institut for Fagsprog, Kommunikation og Informationsvidenskab, Syddansk Universitet.

Zedner, L. (2009). *Security.* Routledge.

Zureik, E. (2003). Theorizing surveillance. The case of the work place. I D. Lyon (Red.), *Surveillance as Social Sorting. Privacy, risk, and digital discrimination* (s. 31-56). New York, New York, USA: Routlegde.