Den digitale dobbeltgænger

Peter Lauritsen
Lektor, Institut for Kommunikation og Kultur – Informationsvidenskab, Aarhus Universitet[1]

Artiklens udgangspunkt er, at digital overvågning (*dataveillance*) indebærer konstruktion og brug af digitale dobbeltgængere, og den forsøger i forlængelse heraf at indkredse dette fænomen. Konkret foreslås, at digitale dobbeltgængere forstås i lyset af begreberne *surveillant assemblages* og *oligoptikon*. Dermed opnås bl.a. en analytisk, neutral forståelse frem for den normative og for det meste kritiske attitude, som traditionelt har præget overvågningsforskningen.

Introduktion

Det er en triviel kendsgerning, at vi lever i et gennemdigitaliseret samfund. Der er, som det ofte udtrykkes, it i alting, hvilket medfører en række smarte teknologier, medier og services, som vi bruger konstant og med stor fornøjelse. Men med informationsteknologiens udbredelse følger også en øget mulighed for overvågning – det der i forskningen ofte betegnes som *dataveillance* (Clarke 1988).

Den forstærkede overvågningsmulighed knytter sig til to forhold: For det første afsætter vi en enorm mængde digitale spor, når vi bruger it (færdes på internettet, bruger vores telefon, betaler med kreditkort etc.). For det andet gør informationsteknologien det muligt for andre at opsamle disse spor, lagre dem i enorme mængder og effektivt søge i dem. Der findes således i dag kartoteker og registre af enhver slags, både i offentligt og privat regi, som indeholder oplysninger om vores bopæl, job, indtægt, sundhed, sociale forhold, forbrug og meget mere.

Med informationsteknologien er overvågningen blevet indvævet i vores hverdag, og det er ikke mindst dette forhold, der gør, at det flere steder fremhæves, at vi i dag lever i et overvågningssamfund (Lauritsen 2011; Lyon 1994; Lyon 2008):

> „It is not just that CCTV may capture our image several hundred times a day, that check-out clerks want to see our loyalty cards in the supermarket or that we need a coded access card to get into the office in the morning. It is that these systems represent a basic, complex infrastructure which assumes that gathering and processing personal data is vital to contemporary living. Surveillance is part of the way we run the world in the twenty-first century" (Lyon 2008, 1).

Når man, som Lyon, definerer overvågning som „gathering and processing personal data", opstår der en tæt kobling til brugen af it, der netop er karakteriseret ved effektivt at kunne indsamle og behandle information. Med informationsteknologien øges overvågningsmuligheden, hvilket rejser en række udfordringer i forhold til, hvordan vi kan og bør gebærde os, men samtidig udfordres den udbredte forståelse, at overvågning næsten per automatik truer vores privatliv, autonomi og frihed, og at bevægelsen mod øget overvågning følgelig må give anledning til uro. For med udbredelsen følger den indsigt, at selvom overvågning naturligvis kan have negative implikationer, så kan den også kan have modsatte og mere positive konsekvenser, f.eks. i form af bedre service, øget omsorg og velfærd.

Denne dobbelthed er erkendt flere steder i overvågningsforskningen og har medført et behov for at udvikle analytiske overvågningsforståelser, som ikke automatisk hæfter sig op på en overvågningskritik, men som gør det muligt at se nuanceret på overvågning som dybt integreret i det samfund, vi lever i (Gad & Lauritsen 2009; Lyon 2006).

Formålet med denne artikel er netop at bidrage til udviklingen af analytiske og ikke-normative overvågningsforståelser. Omdrejningspunktet er den digitale

overvågning, og hovedargumentet vil være, at et særligt kendetegn ved denne er *en løbende produktion og brug af digitale dobbeltgængere*. Disse dobbeltgængere opstår, når myndigheder eller firmaer konsulterer registreringer om os for bedre at kunne vurdere vores helbred, købekraft, sociale status etc. F.eks. lytter hospitalslægen ikke kun til den patient, der sidder foran ham, men kigger også på de oplysninger, som findes i patientjournalen. Bankrådgiveren undersøger registreringerne om vores økonomi, inden hun bevilger et lån. Politiet tjekker vores straffeattest før ansættelse. Arbejdsgiveren registrerer vores indsats og udbetaler løn derefter. Og SKAT ser på bl.a. indtægt, bopæl, familie og sociale forhold, inden de udsender årsopgørelsen. Vi er på den måde mere end os selv – vi er også vores digitale dobbeltgængere (Deleuze 1992).

At digital overvågning implicerer produktionen af dobbeltgængere er ikke nogen ny indsigt (Clarke 1994, Solove 2004). Men som indikeret tilknyttes de ofte en bekymret overvågningsforståelse, der ikke har tilstrækkeligt blik for, at overvågning er et multifacetteret fænomen, som både kan have destruktive og konstruktive konsekvenser.

I forlængelse heraf argumenterer artiklen for, at digitale dobbeltgængere ikke skal begribes normativt, men tværtimod analytisk. Konkret foreslås, at den digitale dobbeltgænger forstås i lyset af Haggerty og Ericsons analyse af det Deleuze-inspirerede *surveillant assemblages* samt Latours begreb om *oligoptikon* (Haggerty & Ericson 2000; Latour 2005; Latour & Hermant 2004). En væsentlig konsekvens af dette er, at dobbeltgængerne betragtes som lokale begivenheder og som et resultat af netværksarbejde. Således opstår dobbeltgængeren først, idet lægen bringer oplysninger i patientjournalen og prøvesvar i relation til patientens aktuelle symptomer og udsagn. Samtidig fremhæver begrebet overvågningens (og dermed dobbeltgængerens) skrøbelighed og afgrænsethed. Endelig, som en vigtig implikation, stilles overvågningens indhold åbent. Overvågning er ikke kun kontrollerende og frihedsberøvende; den kan også være frisættende og velfærdsskabende.

Artiklen er disponeret på følgende måde. Først beskrives begrebet *dataveillance,* som er den lidt kedelige betegnelse for digital overvågning, der ofte anvendes i forskningen. Dernæst introduceres den digitale dobbeltgænger, og der gives nogle eksempler på dens udbredelse. Endelig gøres der i den tredje del et forsøg på teoretisk at indfange digital overvågning og produktionen af dobbeltgængere. Artiklen afsluttes med en diskussion.

Dataveillance

Dataveillance betegner den særlige overvågning, som informationsteknologiens spredning giver anledning til. Ofte tilskrives termen Roger Clarke, som analyserede begrebet sidst i firserne (Clarke 1988), men faktisk er det noget ældre. Allerede i 1973 skriver Donald R. Davis:

> „The computer and the related sciences of cybernetics permit the manipulation and management of vast quantities of disparate bits of information and afford government officials the ability to conduct 'dataveillance' (review presently stored information on a particular subject) for the purpose of retrieving, collating or evaluating those bits of information relevant to the subject of the records check" (Davis i Genosko & Thompson 2006, 125).

Det er informationsteknologien, der gør det relevant at tale om *dataveillance*. I en ofte refereret artikel fra 1988 hæfter Clarke sig således ved de lagrings- og søgemuligheder, som informationsteknologien medfører. Samtidig gør han opmærksom på, hvor let det er at sammenkøre registre og databaser: „Centralized storage, however, is no longer a precondition of the dossier society". Det skyldes, siger Clarke, at de enkelte registre er forbundet til hinanden ved hjælp af et „telecommunications network" (Clarke 1988).

Det var i 1988. Og som bekendt har informationsteknologien udviklet sig hastigt siden da. Computerne er blevet mange gange kraftigere. Lagringskapaciteten er mangedoblet. Internettet er blevet en del af vores dagligdag. Vi går alle rundt med tablets og mobiltelefoner. Og informationsteknologi bygges ind i biler, legetøj, ure, elmålere og alt muligt andet. En konsekvens af denne udvikling er, at det kun giver begrænset mening at tale om *dataveillance* som en særlig form for overvågning, der adskiller sig fra f.eks. biometrisk overvågning eller videoovervågning. Der er masser af informationsteknologi i f.eks. automatisk ansigtsgenkendelse eller registrering af fingeraftryk, ligesom overvågningskameraerne er digitale, billederne opbevares på store harddiske, og man kan lave digitale søgninger. Selvom informationsteknologien kan spille en større eller mindre rolle, må man således konstatere, at *dataveillance* snarere er et aspekt ved al overvågning end en bestemt type. Overvågningen er i sandhed blevet digital (Solove 2004).

Tilbage i 1988 bemærker Clarke, at den digitale overvågning giver nye muligheder. Den kan selvfølgelig være rettet mod bestemte individer, som menes at udgøre en sikkerhedsrisiko, eller som man gerne vil sælge ydelser eller varer til. Men digitaliseringen understøtter også en masseovervågning, som ikke udspringer af en specifik mistanke mod nogle bestemte personer, eller som måske

ikke engang har et specificeret formål. Netop dette er blevet et iøjnefaldende kendetegn ved nutidens overvågning. Andrejevic og Gates citerer f.eks. en CIA-chef for det følgende:

> „The value of any piece of information is only known when you can connect it with something else that arrives at a future point in time… Since you can't connect dots you don't have, it drives us into a mode of, we fundamentally try to collect everything and hang on to it forever" (Andrejevic & Gates 2014, 185).

I dag knytter *dataveillance* således også an til de forhåbninger, mange nærer til udnyttelsen af *big data* (Andrejevic & Gates 2014; Lyon 2014). Enorme mængder af data indsamles og lagres, og først derefter starter en jagt på mistænkelige mønstre og afvigelser, som i nogle tilfælde kan føre til en mere personrettet overvågning. Overvågningens sindbillede bør således ikke så meget være overvågningskameraet, der i realtid følger mistænkelige personer for at tjekke deres færden, men nærmere den digitale indsamling af informationer om enhver borger og den senere organisering, profilering og udvælgelse af interessante hændelser og personer.

Oligoptiske dobbeltgængere

Det er i forhold til denne 'databasering' af overvågningen (både den personrettede og masseovervågningen), at det bliver relevant at tale om eksistensen af en digital dobbeltgænger. Roger Clarke bruger betegnelsen *digital persona*, som han definerer på følgende måde:

> *„The digital persona is a model of an individual's public personality based on data and maintained by transactions, and intended for use as proxy for the individual"* (Clarke 1994, 2. Kursivering i original).

Skattefastsættelse er et oplagt eksempel. Tidligere måtte enhver voksen dansker samle dokumenter og lave udregninger og indberette til skatteväsenet. I dag trækker SKAT langt de fleste oplysninger ud af eksisterende databaser og gør dermed det meste af arbejdet for os. I denne proces dannes en digital dobbeltgænger, som gør det muligt at fastsætte, hvor meget vi skal betale i skat. Som nævnt sker noget lignende, når en læge diagnosticerer en patient. Dette sker selvfølgelig ofte ved, at lægen taler med og føler på patienten, men det sker også og måske især ved, at lægen kigger på prøvesvar, tidligere sygdomme, medicinforbrug etc., som alt sammen er registreret i den elektroniske patientjournal. Dermed har patienten i sin journal en digital dobbeltgænger, der agerer som proxy for individet.

At der oprettes registre med personlige oplysninger, er ikke nyt (Pedersen 2014), men med digitaliseringen sker der et kvantespring, som netop gør dannelsen af dobbeltgængere til et særligt kendetegn ved det overvågningssamfund, vi lever i. Daniel Solove udtrykker det på følgende måde:

> „Digital technology enables the preservation of the minutia of our everyday comings and goings, of our likes and dislikes, of who we are and what we own. It is ever more possible to create an electronic collage that covers much of a person's life – a life captured in records, a digital person composed in the collective computer networks of the world" (Solove 2004, 1).

Solove viser i en amerikansk kontekst, hvordan denne form for overvågning dominerer inden for en række felter og benyttes af både offentlige myndigheder og private virksomheder. Selvom der er visse forskelle, bl.a. i kraft af de nationale lovgivninger, er der ingen tvivl om, at den digitale overvågning og produktion af dobbeltgængere også er udbredt i Danmark.

Det kan man f.eks. se i en række praksisser, som er etableret for at tage vare på vores sikkerhed. I Danmark registreres oplysninger om alle telefonopkald, og hvis politiet har mistanke til en bestemt person, kan de få adgang til dette register og dermed få indsigt i, hvordan den mistænktes telefon er blevet brugt, og hvor den har befundet sig. I nogenlunde samme boldgade har Edward Snowden afsløret, hvordan især den amerikanske efterretningstjeneste NSA udfører en verdensomspændende overvågning af elektronisk kommunikation (Greenwald 2014; Lyon 2014; se også Haggerty & Gazso 2005). Overvågningen udføres efter mottoet „collect it all", hvilket ikke er noget beskedent formål, når det er den samlede mængde af information i verden, vi taler om (Greenwald 2014). I *princippet* giver de mange indhøstede data mulighed for, at NSA (og andre efterretningstjenester) kan lave ret nuancerede personprofiler, men på trods af Snowdens afsløringer ved vi meget lidt om, hvordan informationerne bliver brugt.

Brugen af digitale dobbeltgængere er også tydelig i kommercielle praksisser. En af de mest udbredte forretningsmodeller på internettet er således at kommercialisere viden om købere og brugere. Ved at stille gratis services til rådighed får f.eks. Facebook og Google adgang til brugernes personlige informationer, som lagres og danner

grundlag for mere personaliserede reklamer og ydelser (Palmås 2011). Men igen er pointen, at disse services er baseret på brugerens digitale spor.

Endelig kan man som et tredje eksempel pege på velfærdsstaten som ramme for et væld af digitale overvågningstiltag med tilknyttet produktion af digitale dobbeltgængere. Som nævnt baserer skatteforhold og sundhedsarbejde sig i vid udstrækning på digitale repræsentationer af borgeren (Lupton 2012). Det samme gør tildelingen af sociale ydelser og en række andre forhold, som står centralt i velfærdsstatens virke. En væsentlig krumtap i dette arbejde er CPR og personnummeret, som i hvert fald i en dansk kontekst fungerer som nøglen til det meget store antal registre, som alle borgere er repræsenteret i (Lauritsen 2011).

Som disse eksempler viser, opererer de digitale dobbeltgængere således ikke kun i forholdet mellem borger og stat, men bruges også af private virksomheder. De knytter sig heller ikke alene til opretholdelsen af sikkerhed, lov og orden, men også til velfærd, omsorg og i nogle situationer også til underholdning (Albrechtslund & Dubbeld 2005). En første erkendelse er således, at produktionen af digitale dobbeltgængere følger den digitale overvågning ud i alle hjørner af vores tilværelse.

På tværs af den endnu ret sparsomme litteratur, som engagerer sig i udfoldede diskussioner om overvågning og digitale dobbeltgængere, kan man fremdrage nogle væsentlige punkter, som yderligere medvirker til at indkredse dobbeltgængerens natur (Clarke 1994; Solove 2004).

Det ene er, at en digital dobbeltgænger er en dynamisk konstruktion. I en diskussion af dobbeltgængere inden for sundhedsvæsenet siger Lupton:

> „While the abstracted 'data-double'… may be categorised as a virtual cyberbody, this data-double feeds back information to the user in ways that are intended to encourage the user's body to act in certain ways. The flow of information, therefore, is not one-way or static: it is part of a continual loop of the production of health-related data and response to these data" (Lupton 2012, 237).

I denne og mange andre situationer er der således ikke tale om, at dobbeltgængeren konstrueres og derefter blot ligger passivt hen. Tværtimod føjes der løbende nye informationer til, ligesom dobbeltgængeren kan virke tilbage på subjektet. I dette tilfælde i form af recepter og øvelser, i andre tilfælde i form af f.eks. økonomiske råd eller restriktioner eller som forbud mod at flyve eller bevæge sig bestemte steder hen. Det er ikke sikkert, at dobbeltgængeren virker tilbage på individet på denne måde, men muligheden foreligger.

Et andet forhold er, at selvom digitale dobbeltgængere konstrueres på baggrund af afsatte spor og således er historiske konstruktioner, er målet ofte at kunne forudsige fremtidige handlinger og hændelser (Solove 2004). Efterretningstjenesterne gennemsøger enorme mængder data for at kunne afværge et terrorangreb, før det sker. De store firmaer vil forudsige vores behov, måske endda skabe dem, for bedre at kunne sælge os ydelser og varer. Og sundhedsvæsenet vil gerne kunne forudsige, at bestemte sygdomme opstår, og dermed sætte ind med forebyggende behandling.

Endelig for det tredje kan dobbeltgængeren udmærket blive dannet, uden at vi ved det (Solove 2004). Der er med andre ord mulighed for, at der et eller andet sted sidder nogen og tegner profiler af os – for at hjælpe eller udnytte os, for at sælge os varer og ydelser eller for at sikre sig, at vi ikke er kriminelle eller udgør en sikkerhedsrisiko. Og selv i de situationer, hvor vi faktisk er vidende om konstruktionen, kan det være vanskeligt for os at gøre noget ved det. Man kan selvfølgelig kryptere sin kommunikation, og man bestemmer selv, hvilke informationer man lægger ud på Facebook. Måske har man ligefrem en bevidst strategi for selvfremstillingen. Til gengæld har man langt ringere kontrol over, hvor informationerne ender, og man er sikkert heller ikke klar over, efter hvilke algoritmer data behandles, og derfor har man kun begrænset mulighed for at påvirke, hvordan den digitale dobbeltgænger dannes og kommer til at se ud (Clarke 2014; Lyon 2014).

Som nævnt optræder begrebet om den digitale dobbeltgænger (i forskellige variationer) relativt hyppigt i overvågningslitteraturen. Men desværre nævnes det ofte kun en passant og uden grundige analyser af, hvori dobbeltgængeren består, hvordan den dannes, hvordan den anvendes og med hvilke implikationer.

En undtagelse fra dette overordnede indtryk er imidlertid Clarkes analyser af *dataveillance* og *digital personas* (Clarke 1988; 1994). Et gennemgående tema i dette arbejde er en udtalt bekymring for de konsekvenser, som konstruktionen af digitale dobbeltgængere har. Godt nok understreger Clarke, at han ikke ser overvågning som noget negativt, men alligevel sporer man en tydelig pessimisme: „Nevertheless, dataveillance is, by its very nature intrusive and threatening" (Clarke 1988, 506). Clarke nævner blandt andet:

- Et problem er validiteten af de data, som opbevares. Man kan opleve, at data vedrører en anden person, eller at de bruges i en kontekst, hvor de ikke giver mening.

- Det er heller ikke altid klart, hvorfor der kastes mistanke på en person – nogle gange sker det på grund af en bestemt algoritme, som man ikke kan få indsigt i.
- Det er dem, 'der stikker ud', der mistænkes. Men ikke alle idiosynkrasier er ulovlige, og det kan være vanskeligt at overbevise bureaukratiet om, at selvom man ikke følger normalen, så bør man ikke være under mistanke.
- De data, som gemmes i registrene, bliver måske ikke misbrugt af en demokratisk regering, men de kan være et effektivt redskab i hænderne på et fremtidigt totalitært regime.

Dårlig datakvalitet, misfortolkninger, mistillidskultur, muligheder for et totalitært regime er således blandt de risici, der følger med den digitale overvågning og den tilhørende dobbeltgænger, hvis man følger Clarke. På et mere principielt niveau siger han:

> „A digital persona is a model of an individual, and hence a simplified representation of only some aspects of the reality. The efficacy of the model depends on the extent to which it captures those features of the reality which are relevant to the model's use. As with any modeling activity, it suffers the weaknesses of the reductionist approach: individuals are treated not holistically, but as though a relatively simple set of data structures was adequate to represent their pertinent characteristics" (Clarke 1994, 4).

Clarkes bekymrede indstilling til den digitale dobbeltgænger opstår, fordi han knytter dobbeltgængeren til en overvågningsforståelse, der netop betoner overvågningens mulige negative implikationer – altså en forståelse, hvor overvågning i bund og grund ses som en trussel mod individets frihed, autonomi og *privacy*. At overvågning lige så vel kan have andre og mere positive virkninger, overses her og i mange andre sammenhænge.

Oligoptisk overvågning

Den normative (og bekymrede) overvågningsforståelse er langt fra noget særsyn. Tværtimod baserer diskussioner af overvågning sig ofte på metaforer og begreber, der vægter overvågningens totalitære og undertrykkende aspekter (Albrechtslund 2008). I mange tilfælde er det således muligt at trække linjer fra aktuel forskning til George Orwells roman *1984* og dens beskrivelser af Big Brothers styre, der undertrykker kærlighed og frihed og bruger avanceret overvågningsteknologi til at opretholde dette styre (Orwell 2007). Mere eksplicitte er imidlertid referencerne til Foucaults analyse af panoptikon, hvor læsningerne ofte vægter disciplineringens negative implikationer og den konstante, ubehagelige overvågning, som fangerne i det panoptiske fængsel er udsat for (Bentham & Bozovic 1995; Foucault 1977; Gad & Lauritsen 2009). Om denne normative attitude inden for overvågningsforskningen siger Kevin Haggerty:

> „Surveillance studies replicate this normative orientation. The approach of many surveillance scholars involves a form of hermenutics of suspicion whereby new developments are read negatively as involving inevitable and often cunningly devious expansions and intensifications of surveillance in the service of social control. Consequently, surveillance initiatives are routinely presented as raising disconcerting civil libertarian issues. Such studies are important, but in terms of developing an appreciation for the operation of the totality of contemporary surveillance, they are also severely limited. Once we recognize the incredible range of projects in which surveillance is deployed, it is apparent that surveillance studies tend to neglect surveillance practices that might be accepted as a positive development" (Haggerty 2006, 35).

Retfærdigvis skal det imidlertid tages med, at der i de senere år er dukket konceptualiseringer og begreber op, som netop forsøger at udvikle mere nuancerede overvågningsforståelser (Aas et al. 2009; Lyon 2006). Et tydeligt eksempel på dette er Lyons beskrivelse af overvågning som et Janusansigt. På den ene side lurer faren for kontrol og undertrykkelse. På den anden ønsket om at anvende overvågningen som del af en omsorgspraksis (Lyon 1994; 2007). Forældre overvåger deres børn for omsorgsfuldt at tage sig af dem og bruger i den forbindelse f.eks. babyalarmer og apps på mobiltelefoner, men spørgsmålet er, hvornår denne overvågning slår over til at blive kontrollerende og uhensigtsmæssig – altså fratager børnene et nødvendigt frirum. På lignende vis drager velfærdsstaten omsorg for sine borgere, men udsættes i den forbindelse for kritik af, at omsorgen ikke er tilstrækkelig omfattende eller modsat for, at der ikke længere er tale om omsorg, men om kontrol og overskridelse af borgernes privatliv. Hvorvidt en given overvågningspraksis er omsorgsfuld eller kontrollerende er således ikke altid enkelt at afgøre, men ikke desto mindre er erkendelsen vigtig: Overvågning har også tydelige omsorgsfulde aspekter.

Lyons diskussion af overvågningens omsorgsrelaterede potentiale peger ikke så meget på behovet for endnu

et normativt overvågningsbegreb, nu blot med modsat fortegn, eller på en forståelse af digitale dobbeltgængere som per definition værende enten konstruktive eller destruktive. Behovet er nærmere begreber og forståelser, der fremhæver, at overvågning netop ikke skal indholdsbestemmes på forhånd, men tilgås analytisk og åbent.

Et velkvalificeret bud på et sådant perspektiv findes hos Haggerty og Ericson (2000), der med inspiration fra Deleuze har foreslået *surveillant assemblage* som en ressource for overvågningsforskningen. Dette skal forstås som et heterogent patchwork eller en mosaik, som forbinder mennesker, artefakter, teknologi etc. Samtidig signalerer begrebet proces fremfor produkt:

> „To speak of *the* surveillant assemblage risks fostering the impression that we are concerned with a stable entity with its own fixed boundaries. In contrast, to the extent that the surveillant assemblage exists, it does so as a potentiality, one that resides at the intersections of various media that can be connected for diverse purposes" (Haggerty & Ericson 2000, 609).

Et 'overvågningsassemblage' er altså at forstå som en proces, hvor forskellige data og processer forbindes, hvorved den digitale dobbeltgænger opstår. Haggerty og Ericson beskriver processen på denne måde: „The observed body is … broken down by being abstracted from its territorial setting. It is then reassembled in different settings through a series of data flows" (Haggerty & Ericson 2000, 611). Med andre ord medfører overvågning, at data om individet fjernes og gemmes et andet sted og i en anden kontekst end der, hvor de blev udtaget. Skulle der opstå behov for det, kan disse data findes frem igen, de kan eventuelt kobles til andre data, og resultatet er, at der dannes en digital dobbeltgænger. Om denne så er god eller slet, effektiv eller ineffektiv, siger begrebet ikke noget om. Sådanne spørgsmål må afgøres gennem specifikke empiriske undersøgelser.

Denne skitse kan udvikles yderligere ved at inddrage begrebet om *oligoptikon*, der er udviklet af Bruno Latour (Latour & Hermant 2004; Latour 2005). Oligoptikon kan siges at være aktørnetværksteoriens (ANT) overvågningsbegreb og deler dermed tydelige fællestræk med *surveillant assemblages*, bl.a. fordi også ANT har tråde til Deleuzes arbejde.

Man kan sammenfatte den oligoptiske overvågningsforståelse i følgende punkter: Overvågning er 1) et resultat af netværksarbejde, 2) principielt skrøbelig og 3) afgrænset. Endelig er begrebet analytisk orienteret og åbent for, at overvågning kan have mangfoldige implikationer (for en grundigere gennemgang se f.eks. Bøge 2015; Gad & Lauritsen 2009).

At overvågningen er et resultat af netværksarbejde, indebærer, at forskellige aktører (det være sig mennesker eller teknologier) arbejder sammen på en mere eller mindre velkoordineret måde. F.eks. kræver effektiv videoovervågning, at bl.a. kameraer, politifolk og i virkeligheden også forbryderne hver især bidrager (Lauritsen 2015). Overvågning handler således ikke alene om at se, men i lige så høj grad om at arbejde og konstruere. Pointen er ikke mindst interessant i forhold til den digitale overvågning. Registre etableres, udvides og konsulteres, men resultatet er ikke, at man kan iagttage en levende krop, men derimod en repræsentation af personen, altså en digital persona eller en digital dobbeltgænger (Los 2006).

Det forhold, at overvågningen er netværksproduceret, tilfører den en principiel skrøbelighed, eller som Latour udtrykker det, „the tiniest bug can blind oligoptica" (Latour 2005, 181). Hvis koordineringen af aktørernes samarbejde ikke er tilstrækkelig, eller en aktør ikke udfører sit arbejde, vil det forandre overvågningen.

For konstruktionen af den digitale dobbeltgænger betyder det, at hvis de rigtige ressourcer er til rådighed, og netværksarbejdet lykkes, så kan man etablere en dobbeltgænger, som kan udfylde den rolle, som den var tiltænkt. Men succesen er ikke garanteret, fordi dobbeltgængeren netop kræver, at arbejde koordineres. Er der ikke adgang til et register, eller er de indtastede data forkerte, er det ikke sikkert, at dobbeltgængeren fungerer efter hensigten. Dette kan man i nogle situationer vælge at ignorere, i andre situationer må man starte forfra eller ligefrem opgive.

Et tredje kendetegn ved et oligoptikon er, at overvågningen ikke er total, men lokal og begrænset. Herved adskiller den oligoptiske overvågningsforståelse sig fra både Orwells Big Brother og panoptikon. I begge tilfælde ses overvågeren som altseende. Man kan ikke gemme sig for Big Brother, uanset hvor meget man forsøger, og hele ideen i det panoptiske fængsel er, at fangerne ikke har noget sted at skjule sig. Anderledes med et oligoptikon:

> Oligoptica [...] do exactly the opposite of the panoptica: they see much too little to feed the megalomania of the inspector or the paranoia of the inspected, but what they see, they see it well... (Latour 2005, 181).

Selvom den oligoptiske overvågning således er afgrænset og fokuseret, kan den udmærket være effektiv. Lægen bliver i stand til at behandle patienten, skatteinddrivelsen bliver rimelig, og forbryderen fanges. Men det sker ikke, fordi overvågeren ser alt, men fordi det er lykkedes at

etablere en dobbeltgænger med tilstrækkelige karakteristika.

Endelig som et fjerde kendetegn indebærer den oligoptiske forståelse en analytisk åbenhed over for overvågningens formål og konsekvenser. Det udelukkes ikke, at overvågningen kan være kontrollerende og undertrykkende, men den kan lige så vel være omsorgsfuld eller underholdende (Albrechtslund & Dubbeld 2005). Om overvågningen er det ene eller det andet (eller sandsynligvis flere ting på en gang), må afgøres gennem en konkret, empirisk analyse.

Med de ovenstående kendetegn tilbyder surveillant assemblages og oligoptikon en interessant kvalificering af den digitale overvågning og den tilknyttede produktion af digitale dobbeltgængere. Sidstnævnte opstår således i specifikke situationer, når bestemte ressourcer trækkes sammen og danner en mere eller mindre stabil repræsentation af os. Dette sker ikke en gang for alle, men kan tværtimod bedre forstås som en række paralleller processer, hvor dobbeltgængere løbende konstrueres i forskellige sammenhænge med forskellige formål. Nogle bliver skabt i sikkerhedspraksisser, andre af kommercielle firmaer og endnu andre på vores vej gennem velfærdssamfundet.

Det er klart, at vi skal følge disse processer med en kritisk opmærksomhed, men en af styrkerne ved den oligoptiske overvågningsforståelse er, at den ikke som udgangspunkt betragter de digitale dobbeltgængere som en trussel. De er tværtimod et vilkår og en forudsætning for det samfund, vi lever i.

Diskussion

Udgangspunktet for denne artikel har været, at med den øgede digitalisering følger også en øget overvågning. Vi afsætter digitale spor, som kan samles op, analyseres og danne grundlag for interventioner af den ene eller den anden art. Heraf følger opfordringen til at rette opmærksomheden mod den produktion af digitale dobbeltgængere, som overvågningen giver anledning til.

Dobbeltgængerne konstrueres ved, at ressourcer af forskellige typer føjes sammen. Når vores skat beregnes, sker det ved, at oplysninger om arbejdsforhold, boligsituation, kørsel, økonomi og meget andet trækkes sammen i et billede af os, hvilket gør det muligt at handle i forhold til netop dette formål. På samme måde bruger lægen oplysninger fra journaler, forskning, laboratorier og eventuelt patientens egne oplevelser til at danne en dobbeltgænger, som kan medvirke til at stille en diagnose. Dobbeltgængeren kan så virke tilbage på patienten i form af råd og vejledning til, hvad han eller hun skal og bør foretage sig.

Hvordan man analytisk tilgår den digitale dobbeltgænger afhænger af, hvilken overvågningsforståelse man knytter den til. Her vil et udgangspunkt i klassiske overvågningsforståelser som Big Brother og panoptikon medføre, at dobbeltgængeren mødes med mistro og bekymring. Der er noget uafvendeligt og farligt ved, at spor opsamles og sættes sammen til dobbeltgængere. Selvom der absolut er grund til at fastholde en kritisk opmærksomhed, overser sådanne forståelser imidlertid, at overvågning også har en række 'positive' implikationer; de digitale dobbeltgængere bruges også i velfærdssammenhænge og til at sikre tryghed.

En af styrkerne ved den oligoptiske overvågningsforståelse er, at den undlader en gang for alle at indholdsbestemme overvågningen. I stedet peger den på nogle overordnede vilkår for overvågningen og de dobbeltgængere, som knytter sig til den: Der kræves arbejde, overvågningen er principielt skrøbelig, og den er ikke total, men afgrænset. Det betyder, at vi ikke skal frygte den digitale overvågning som sådan, men i stedet engagere os i grundige, empiriske analyser af den.

Sådanne analyser er nødvendige, for den udbredte og stadig mere gennemtrængende digitale overvågning har konsekvenser. En af dem er, at den medfører en sortering af mennesker. For nogle åbner der sig døre, fordi deres digitale dobbeltgænger har bestemte kendetegn. Andre er ikke så heldige, og dørene lukker i. Om dette siger Lyon:

> „The surveillance concerned is a form of social sorting, of categorizing persons and groups in ways that appear to be accurate, scientific, but which in many ways accentuate difference and reinforce existing inequalities" (Lyon 2001, 173).

Lyons pointe er, at de algoritmer og kategorier, som dobbeltgængeren baseres på, ikke er neutrale, men tværtimod udtrykker fordomme, politik og etiske forestillinger. Dette er en vigtig erkendelse, fordi det retter fokus mod disse kategorier, som nødvendigvis må udtages til inspektion. For Lyon er det således vigtigt, at forskeren (eller enhver anden) løbende stiller spørgsmål til den overvågningspraksis, som de digitale dobbeltgængere er en del af.

At se den digitale dobbeltgænger som et konstrueret oligoptikon, der både er skrøbeligt og begrænset, tvinger netop opmærksomheden hen imod den specifikke overvågningspraksis. Begrebet indeholder en åbenhed over for, at overvågning kan have totalitære og undertrykkende konsekvenser. Den kan imidlertid lige så vel være omsorgsfuld og frihedsskabende. Men en vigtig oligoptisk pointe er, at man ikke én gang for alle skal tage stilling til, om overvågning via digitale dobbeltgængere er det ene eller det andet. Begrebet er ikke normativt, men analytisk og empirisk orienteret. Konsekvensen er

dermed ikke en fast forestilling om overvågningens natur, men et presserende forskningsmæssigt engagement i at undersøge, hvordan og med hvilke konsekvenser digitale dobbeltgængere konstrueres, vedligeholdes, anvendes og eventuelt stedes til hvile.

Litteratur

Aas, KF, Gundhus, HO & Lomell, HM (red.) 2009, *Technologies of In-Security. The Surveillance of Everyday Life*, Routledge, Milton Park.

Albrechtslund, A, & Dubbeld, L 2005, 'The Plays and Arts of Surveillance: Studying Surveillance as Entertainment', *Surveillance & Society*, vol. 3, no. 2/3, pp. 216-21.

Albrechtslund, A 2008, *In the Eyes of the Beholder: Introducing Participation and Ethics to Surveillance*, ph.d.-afhandling, Aalborg Universitet, Aalborg.

Andrejevic, M & Gates, K 2014, 'Big Data Surveillance: Introduction', *Surveillance & Society*, vol. 12, no. 2, pp. 185-96.

Bentham, J & Bozovic, M 1995, *The Panopticon Writings*, Wo Es War, Verso, London ; New York.

Bøge, AR 2015, *Overvågningens DNA. En Aktør-Netværks-Teoretisk Undersøgelse Af DNA I Dansk Politiarbejde*, ph.d.-afhandling, Aarhus Universitet, Aarhus.

Clarke, R 1988, 'Information Technology and Dataveillance', *Communication of the ACM*, vol. 31, no. 5.

Clarke, R 1994, 'The Digital Persona and its Application to Data Surveillance', *The Information Society,* vol. 10, no 2, pp. 77-92.

Clarke, R 2014, 'Promise Unfulfilled: The Digital Persona Concept, Two Decades Later', *Information Technology & People,* vol. 27, no. 2, pp. 182-207.

Deleuze, G 1992, 'Postscript on the Societies of Control', *October,* vol. 59, pp. 3-7.

Foucault, M 1977, *Discipline and Punish: The Birth of the Prison*, Allen Lane, London.

Gad, C & Lauritsen, P 2009, 'Situated Surveillance: An Ethnographic Study of Fisheries Inspection in Denmark', *Surveillance & Society* vol. 7, no. 1, pp. 49-57.

Genosko, G & Thompson, S 2006, 'Tense Theory: The Temporalities of Surveillance', in D Lyon (red), *Theorizing Surveillance. The Panopticon and beyond*, Willan Publishing, Cullompton, Devon.

Greenwald, G 2014, *Overvåget. En Insiderberetning Om Edward Snowden, NSA Og Den Amerikanske Overvågningsstat*, Informations forlag, København.

Haggerty, KD & Ericson, RV 2000, 'The Surveillant Assemblage', *British Journal of Sociology*, vol. 51, no. 4, pp. 605-22.

Haggerty, KD 2006, 'Tear down the Walls: On Demolishing the Panopticon' in D Lyon (red), *Theorizing Surveillance. The Panopticon and beyond*, Willan Publishing, Cullompton, Devon.

Haggerty, KD & Gazso, A 2005, 'Seeing Beyond the Ruins: Surveillance as a Response to Terrorist Threats', *Canadian Journal of Sociology*, vol. 30, no. 2, pp. 169-87.

Latour, B & Hermant, E 2004, *Paris: Invisible City*. Tilgået 6. august 2015 på: http://www.bruno-latour.fr/sites/default/files/downloads/viii_paris-city-gb.pdf

Latour, B 2005, *Reassembling the Social: An Introduction to Actor-Network-Theory*, Oxford University Press, Oxford.

Lauritsen, P 2011, *Big Brother 2.0. Danmark Som Overvågningssamfund*, Informations forlag, København.

Lauritsen, P 2015, 'Identifying the Perpetrator: An Ethnographic Study of CCTV in Police Work', in I van der Ploeg & J Pridmore (red.), *Digitizing Identities*, Routledge, Oxon.

Los, M 2006 'Looking into the Future: Surveillance, Globalization and the Totalitarian Potential', in D Lyon (red), *Theorizing Surveillance. The Panopticon and beyond*, Willan Publishing, Cullompton, Devon.

Lupton, D 2012, 'M-Health and Health Promotion: The Digital Cyborg and Surveilance Society', *Social Theory & Health,* vol. 10, no. 3, pp. 229-44.

Lyon, D 1994, *The Electronic Eye : The Rise of Surveillance Society*, University of Minnesota Press, Minneapolis.

Lyon, D 2001, 'Facing the Future: Seeking Ethics for Everyday Surveillance', *Ethics and Information Technology*, vol. 3, pp. 171-81.

Lyon, D (red.) 2006, *Theorizing Surveillance: The Panopticon and beyond*, Willan Publishing, Culompton.

Lyon, D 2007, *Surveillance Studies : An Overview*, Polity, Cambridge.

Lyon, D 2008, *Surveillance Society*, præsentation på Festival del Diritto, Piacenza, Italien, 28. september 2008.

Lyon, D 2014, 'Surveillance, Snowden, and Big Data: Capacities, Consequences, Critique', *Big Data & Society*, vol. 1, no. 2, pp. 1-13.

Orwell, G 2007, *1984*, Gyldendal, København.

Palmås, K 2011, 'Predicting What You'll Do Tomorrow. Panspectric Surveillance and the Contemporary Corporation', *Surveillance & Society, vol.* 8, no. 3, pp. 338-54.

Pedersen, KP 2014, *Kontrol over København. Studier i den sene enevældes sikkerhedspoliti 1800-48*, Syddansk Universitetsforlag, Odense.

Solove, DJ 2004, *The Digital Person. Technology and Privacy in the Information Age*, New York University Press, New York.

Noter

1. Forfatteren ønsker at takke en anonym reviewer samt redaktøren for gode, konstruktive kommentarer.