

Introduktion

Et tværdisciplinært blik på privatliv og overvågning

Overvågning og retten til privatliv har fyldt meget i den offentlige debat det seneste år, internationalt såvel som i Danmark. Edward Snowden's læk af dokumenter fra den amerikanske efterretningstjeneste, der startede i sommeren 2013 og er fortsat i 2014, har for alvor sat spot på stater og efterretningstjenesters adgang til at overvåge deres borgere. Samtidig er det blevet tydeligt, at den øgede digitalisering, de digitale medier, og de allestedsværende kameraer er med til at sætte retten til privatliv under pres.

Formålet med dette særnummer er at sætte fokus på dansk forskning indenfor den brede ramme: privatliv og overvågning. Emnet er bredt og tværdisciplinært i sin natur, og kan angribes på forskellig vis afhængig af ens politiske, epistemologiske, eller etiske ståsted - såvel som fra et juridisk, kulturelt, historisk, teknologisk, eller anden forskningstradition. Dette særnummer vil præsentere nogle af disse mange tilgange til forskning indenfor privatliv og overvågning. Vi håber, at vi med særnummeret kan sætte skub i mere forskning inden for privatliv og overvågning i Danmark, og at forskning i højere grad tænkes ind i tværdisciplinære problemstillinger og miljøer.

Et sted man kunne starte diskussionen af privatliv og overvågning er ved at konstatere, at Danmark på mange måder er et overvågningssamfund. For nogen er det måske en provokerende konstatering, fordi de forbinder overvågningen med en undertrykkende Big Brother, der ved hjælp af teleskærme, tankepoliti og glemselshuller kontrollerer en føjelig befolkning. Men anlægger man en mere nøgtern betragtning, hvor overvågning ikke gives en bestemt normativ værdi, men i stedet forstås som en systematisk ind-

samling af information om nogen eller noget med henblik på at kunne påvirke dette nogen eller noget, så stiller sagerne sig anderledes. Vi kan nu få øje på overvågning og overvågningsteknologi stort set alle steder. Overvågningskameraer filmer os i banker, cafeer og butikker og nogle steder også på gaden. Men vi har også i stigende grad overvågningskameraer derhjemme, i sommerhuset, daginstitutioner, skoler, biblioteker, etc. sådan at vi kan følge med i, hvad der foregår og måske føle os en smule tryggede.

En anden væsentlig overvågningsteknologi er vores mobiltelefon. Vi kan filme politiet, overfaldsmænd og hinanden. Men vi kan også tracke vores ægtefæller og vores børn eller holde øje med vores sundhed, kost og motion. Samtidig holder telefonen øje med, hvor vi er, og der indsamles systematisk oplysninger om vores telefonsamtaler, mailudvekslinger og sms'er. Mobiltelefonen er med andre ord en vigtig overvågningsteknologi i dobbelt forstand. Den giver brugeren mulighed for at overvåge både sig selv og andre, men den giver også andre mulighed for at overvåge os.

Men der er mere endnu. Når vi bruger plastickort registreres det, hvad vi køber og hvor vi befinder os. Med en GPS i firmabilen kan arbejdsgiveren se, om vi kører ad den mest effektive rute. Den personlige kode, som åbner døren ind til lageret, gør det muligt at se, hvem der har været der på hvilke tidspunkter. Cookies på computeren overvåger vores internetbrug. Og så har vi ikke engang nævnt de hundredevis af data samlinger, som indeholder oplysninger om danskernes sundhed, økonomi, sociale forhold, familierelationer, bopæl, kriminelle løbebane og

meget andet. Vi er her registreret efter vores personnummer, og hvis man sammenkører oplysningerne kan man få meget detaljeret viden om hver eneste dansker.

Ovenstående er langt fra en udtømmende liste over den overvågning, som vi udsættes for eller selv udfører. Men den viser, at udsagnet om, at Danmark er et overvågningssamfund i virkeligheden er en trivial konstatering. Overvågningen følger os næsten hele tiden; den er i vores hverdagsliv, i den offentlige debat, og den behandles i film, bøger og teaterstykker. Man kunne med andre ord sige at ovenstående alene er en beskrivelse af det moderne digitale informationsfund; at den måde vi (bevidst eller ubevidst) har indrettet samfundet på har skabt et overvågningsfund. De netværksforbundne teknologier indsamler som default information og data om borgere og forbrugere, når de foretager sig dagligdags ting.

Denne allestedsnærværende overvågning udgør en udfordring for retten til privatliv. Retten til privatliv følger af FN's Verdenserklæring om Menneskerettigheder (1948), der slår fast, 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"¹. En række af FN's konventioner indeholder lignende bestemmelser, der beskytter privatlivet, herunder FN's konvention om civile og politiske rettigheder. Endvidere er retten til privatliv beskyttet i Den Europæiske Menneskerettighedskonvention. Retten til privatliv er ikke absolut, men indgreb skal følge menneskeretlige standarder, herunder have hjemmel i lov og udgøre en nødvendig og proportional foranstaltning.

Det øgede internationale fokus på overvågning medførte i 2013 den første FN resolution om Retten til Privatliv i en Digital Tidsalder.² Resolutionen, der blev vedtaget i december 2013, understreger at retten til privatliv er under pres og at stater har en forpligtelse til at sikre, at national lovgivning der hjemler overvågning er i overensstemmelse med de menneskeretlige standarder på området. Som opfølgning på resolutionen iværksatte FN's Højkommissær for Menneskerettigheder i 2014 en undersøgelse af overvågningsrelateret lovgivning og tilsyn med denne, på tværs af FN's medlemsstater. Undersøgelsen konkluderer blandt andet, at overvågning i stigende grad er normen snarere end undtagelsen; at mange

stater har et mangelfuldt lovgrundlag for deres overvågningsaktiviteter; at de procedurer der skal sikre individets retssikkerhed ofte er for ringe, og at det uafhængige tilsyn med overvågning i mange lande er for svagt. Endvidere fandt Højkommissæren, at private virksomheder i mange tilfælde udnyttes til at give adgang til personoplysninger, uden at de berørte personer informeres om det.³ Højkommissærens fremhæver masseovervågning og generel logning af kommunikationstrafik som særligt problematiske områder; og understreger at efterretningstjenesternes vide adgang til at opsamle data fordrer effektive retssikkerhedsmæssige garantier og tilsyn.

I Danmark kom overvågning endnu en gang på den politiske dagsorden med Se & Hør / Nets sagen i april 2014. Sagen omhandler lækning af personoplysninger fra Nets, der gjorde Se & Hør i stand til at få information om kendte og andre personers brug af kreditkort. Derudover har overvågning og retten til privatliv blandt andet været diskuteret i forbindelse med EU domstolens underkendelse af EU's logningsdirektiv i april 2014⁴, og vedtagelsen af lov om center for Cybersikkerhed i juni 2014.⁵ Tillige har der været en række løbende sager om mangelfuld IT sikkerhed hos offentlige institutioner og private virksomheder, herunder læk af personnumre, hacking af kørekortregisteret, læk af personoplysninger om el-kunder, fejlagtige udleveringer af sundhedsoplysninger med videre.

Som resultat af de mange danske sager nedsatte Folketinget i juni 2014 en parlamentarisk arbejdsgruppe, der skal undersøge mulighederne for en bedre beskyttelse af personoplysninger i offentlige institutioner og private virksomheder.⁶ Arbejdsgruppen har foreløbig valgt at fokusere på tre områder; offentlige myndigheders behandling af personoplysninger, tekniske krav og standarder til fremme af datasikkerhed, samt tilsynet med databeskyttelse i offentlige myndigheder og private virksomheder.

Overvågningen er også - efterhånden - blevet en del af forskningen. I betragtning af overvågningens udbredelse og omfang har forskningsinteressen imidlertid været både tøvende og sporadisk. Det er inden for det juridiske felt, at opmærksomheden har været mest vedvarende bl.a. med fokus på cyber sikkerhed, tv-overvågning, persondatalov og overvågning på arbejdspladser. Inden for datalogien har man først og fremmest arbejdet med at bygge overvågningstekno-

log bl.a. forskellige mobile overvågningssystemer, mens man i informationsvidenskaben i højere grad har været interesseret i at analysere overvågningens karakter og anvendelse. Det er f.eks. sket i større forskningsprojekter om overvågning i politiarbejde og brugen af forskellige tracking-teknologier. Der har også været forskning i overvågningens kulturelle implikationer og der er eksempler på, at idrætsforskere har taget overvågning op.

De forskningsmæssige spørgsmål knyttet til overvågning og privatliv er således langt bredere end spørgsmålet om staters adgang til at overvåge, ikke mindst i en dansk kontekst. Udfordringerne kalder på analyser og forskning fra mange forskellige fagområder, og aktualiserer behovet for tværfaglig udveksling af viden og resultater. Formålet med dette særnummer er at formidle resultater fra forskere, der arbejder med digitalisering, overvågning, og privatliv fra en række forskellige perspektiver.

I dette temanummer præsenterer vi fem forskningsartikler samt en boganmeldelse. Den første artikel, "*Efter indhentet efterretning. Et historisk rids af overvågning i enevældens København*" af Laura Skouvig giver et historisk overblik over hvorledes informationssamfundet og overvågningssamfundet opstår samtidigt. Artiklen viser hvorledes overvågning udgår fra information - etableringen af procedurer for produktion af information, særligt politiets behov for information om borgerne, som samtidig skaber overvågning af borgernes færden. Omdrejningspunktet for Skouvig's analyse er København i begyndelsen af det 19. århundrede. Kristen Veel fortsætter den diskussion i sin artikel, "*Nothing to Hide and Nothing to See. Total Information and the Conditions of Privacy in Jennifer Egan's Black Box*" hvor Veel med udgangspunkt i Egan's Twitter novelle *Black Box* udfolder sammenhængen og relationerne mellem information, overvågning, og det narrative. Hovedpersonen i *Black Box*, den smukke Lulu, er en *overvågningscyborg*, som kan tage billeder, optage video og hente data fra andre teknologier direkte med sin krop og derved skaber muligheden for det totale informationsrum.

Den tredje artikel, Nanna Bonde Thylstrup's "*Archival Shadows. Presence and Privation in Digital Archives*" tager ligeledes et litterært afsæt - Thylstrup bruger H.C. Andersen's eventyr *Skyggen* i sin diskussion af dataskygger; den samlede mængde af

information som en person efterlader igennem sine daglige digitale aktiviteter. I H.C. Andersen's eventyr ender *Skyggen* med at have magt over manden, og på samme måde diskuterer Thylstrup hvorledes dataskyggen må kunne forstås teoretisk såvel som empirisk.

De to sidste artikler i dette særnummer tager fat på de juridiske aspekter af privatliv og overvågning. I "*I en højere sags tjeneste. Afvejningen mellem overvågning og privatliv i en retlig kontekst*" afsøger Lars Bo Langsted og Søren Sandfeld Jakobsen de grundlæggende problemstillinger, regler, principper og hensynsafvejninger der foretages for lovmæssigt at sikre borgeres ret til privatliv. De noterer at "overvågning" ikke som sådan er defineret i lovgivningen og at forholdet mellem retten til privatliv på den ene side og adgangen til overvågning på den anden side er juridisk meget kompleks - og at der inddrages både europæisk og dansk ret i denne afsøgning. I den femte og sidste artikel, "*Overvågning. Kan persondataretten gøre nytte?*", undersøger Peter Blume først begreberne privatliv (eller privathed) og overvågning, for derefter at diskutere hvorledes persondataretten og den kommende EU persondataforordning kan sikre borgeres og forbrugeres privatliv. Blume konkluderer at kun en kombination af retlig regulering, privatlivsvenlig teknologi, samt et højt opmærksomhedsniveau kan sikre privatlivets fred.

Afslutningsvis anmelder Søren Friis bogen "*Liberty and Security*" af Conor Gearty. Gearty diskuterer og analyserer den gængse argumentation om, at forholdet mellem frihed og sikkerhed er et spørgsmål om at finde den rette balance mellem de to.

Til trods for at de seks indlæg i dette særnummer kommer fra forskellige forskningstraditioner, har forskellige formål, og trækker på forskellige teoretiske begrebsrammer deler de en fælles målsætning om at forstå forholdet mellem indsamling af information for at bedre, lette, eller sikre en situation og menneskers liv og samtidig sikre den fundamentale ret til privatliv. Det er situationen i København i begyndelsen af det 19. århundrede; det er problemstillingen i Egan's novelle *Black Box*; det er anskueliggjort med dataskygger som eksempler på den digitale verdens dilemma, og det er fremhævet i gennemgangen af de juriske problemstillinger ved at sikre mod overvågning. Spørgsmålene er mangfoldige og komplicerede, og den omdiskuterede afvejning mellem frihed

og sikkerhed trækker på både teknologiske løsninger og retlig regulering.

Det er vores håb, at dette særnummer af *Nordisk Tidsskrift for Informationsvidenskab og Kulturformidling* kan bidrage til at skabe mere interesse for forskning i privatliv og overvågning i og på tværs af danske forskningsmiljøer. Problemstillingerne omkring privatliv og overvågning bliver kun større i de kommende år i takt med at samfundet og hverdagen gøres stadig mere digital. Tværdisciplinær forskning, der trækker på forskellige forskningstraditioner, kan være med til at give en mere nuanceret forståelse af de mange samfundsmæssige udfordringer, vi står overfor, og deres mulige løsninger.

Noter

1. Jf. FN's Verdenserklæring om Menneskerettighederne - artikel 12.
2. Jf. The Right to Privacy in the Digital Age, Resolution vedtaget på FN's Generalforsamling, 18. december 2013. A/RES/68/167.
3. Jf. The right to privacy in the digital age, Rapport fra FN's Højkommissær for Menneskerettigheder, 30. juni 2014. A/HR/C/27/37.
4. Jf. EU-domstolens dom af 8. april 2014.
5. Jf. Lov om Center for Cybersikkerhed af 25. juni 2014.
6. Beretning afgivet af Kulturudvalget og Retsudvalget den 3. juni 2014.

God læselyst!

Jens-Erik Mai
Københavns Universitet

Peter Lauritsen
Aarhus Universitet

Rikke Frank Jørgensen
Institut for Menneskerettigheder