”In God we trust – all others bring data”[1]

Vor frihed til egne personfølsomme oplysninger på internettet befinder sig i skyggen af terrorovervågningen. Danskerne blev således i 2013 registreret 3,5 billioner(10^{12}) gange på mobil eller internet. Hvad bruger myndighederne disse data til? Hvilke kommercielle interesser er på spil? Og i hvilken grad er friheden til vort privatliv truet?

Indledning

Ikke-indblanding i privatlivet hænger nøje sammen med frihedsbegrebet. Dette vil jeg belyse ved at se på, hvordan bl.a. ”the war against terror” efter 9/11 har ført til misbrug af vore personlige data (en nærmere definition heraf vil jeg komme ind på senere) på internettet. Første skridt er at tage udgangspunkt i Isaiah Berlins todelte definition af frihed i henholdsvis negativ og positiv frihed[2]. Den uddyber dog ikke i særlig grad retten til privatliv. Ronald Dworkin (2002) kommer det lidt nærmere i sin gennemgang af følgerne af anti-terrorlovgivningen, omend han kun i forbifarten nævner faren for datamisbrug. Selv om Lucia Zedner (2005) primært beskæftiger sig med sikring af kriminelles/ terroristers rettigheder, er der nogle af hendes overvejelser, der tilfører begrebet en yderligere dimension og i endnu højere grad Jeroen van den Hoven (2014). Som et lille indskud ser jeg også på Robert A. Dahls begreb om personlig autonomi (1989). Før jeg når til min case – brug og misbrug af personfølsomme oplysninger på nettet – er der dog behov for yderligere en kort bestemmelse af begrebet privatliv, som fremføres af Lou Hodges (2009). Sidstnævnte stammer fra et andet område end filosofien, nemlig fra massemedie-etik.

Men først vil jeg, som nævnt, koncentrere mig om Berlins syn på frihed, der også kort omtales i relation til individuel ’status’ og demokrati. Vigtigst er dog hans todelte definition af frihedsbegrebet.

To frihedsbegreber

At tvinge et menneske er at fratage ham frihed, men frihed fra hvad, spørger Berlin retorisk. Han vælger at se på to, politiske udlægninger af frihedsbegrebet: Den første, som han kalder *negativ* frihed, er svaret på spørgsmålet:

> ”*What is the area within which the subject – a person or group of persons is or should be left to do or be what he is able to do or be, without interference by other persons*”[3].

Her er der tale om frihed som den personlige, valgte udfoldelse uden indblanding. Frihed som noninterferens. Den anden, *positiv* frihed eller frihed til noget, er svaret på følgende spørgsmål:

---

[1] Viktor Mayer-Schönberger og Kennet Cukier, 2013: Big Data: 166, brugt som mantra, der bl.a. høres i Silicon Valley
[2] Isaiah Berlin, 1969: Two Concepts of Liberty in Four Essays on Liberty
[3] Ibid, 1969: 2

> *What, or who, is the source of control or interference that can determine someone to do, or be, this rather than that"*[4].

Altså en situation, hvor man ikke længere er enerådende, men hvor andre har frihed til at gribe ind og tage beslutninger på ens vegne. For det kan sommetider være retfærdigt at tvinge mennesker på vegne af et fælles mål eller for ens egen skyld, om end der heri også ligger en fare for paternalisme, dvs. en formynderisk holdning om, hvad der er bedst for den enkelte borger. I begge begreber – positivt som negativt – kan man tolke det som den enkeltes integritet og grænserne herfor.

Demokrati

Berlin foretager et opgør med 'de gamle liberale' (blandt andre John Stuart Mill) og deres syn på positive frihed. Han understreger, at der ikke er nogen nødvendig forbindelse mellem individuel frihed og et demokratisk styre; tværtimod finder han denne forbindelse spinklere end fortalere for begge gør. Ifølge ham er der en logisk forskel på hvem, der regerer mig og hvor langt en regering blander sig. "*It is in this difference that the great contrast between the two concepts of negative and positive liberty, in the end, consist*"[5].

Og senere:

> *"Democracy may disarm a given oligarchy, a given privileged individual or set of individuals, but can still crush individuals as mercilessly as any previous ruler. An equal right to oppress – or interfere – is not equivalent to liberty"*[6].

I begrebet frihed ligger at være sin egen herre; at blive "genkendt", være medlem af et samfund, føle at man hører til og er et rationelt individ:

> *"I am not seeking equality of legal rights, nor liberty to do as I wish (..) but a condition in which I can feel that I am, because I am taken to be, a responsible agent, whose will is taken into consideration because I am entitled to it, even if I am attacked and persecuted for being what I am or choosing as I do"*[7].

Berlin vender flere gange tilbage til denne søgen efter status, efter dette at være nogen. For ønsket om status og genkendelse netop som individ kan hverken forstås som individuel frihed i udelukkende dens negative eller positive betydning af ordet. Ønsket om denne genkendelse skal derimod søges i forening, tættere forståelse, det at dele interesser, et liv i fælles afhængighed og fælles ofre, som Berlin kalder det. Selv er han dog ikke i tvivl om blandingsforholdet: *"No doubt every inter-*

[4] Ibid: 2
[5] Ibid: 7
[6] Ibid: 27
[7] Ibid: 22

pretation of the word 'liberty', however unusual, must include a minimum of what I have called 'negative' freedom [8].

Det er således ikke frihed at gøre, hvad der er irrationelt, dumt eller forkert. Men ønsket om frihed til at leve som man vil, må vægtes mod kravet om andre værdier som lighed, retfærdighed, lykke eller *"security, or public order are perhaps the most obvious examples. For this reason, it cannot be unlimited"*[9].

Her er Berlin inde på netop sikkerhed og offentlig orden, der i en bredere betydning *kunne* rumme også datasikkerhed. Men det nævner han ikke, hvilket er forståeligt, da artiklen udkom i 1969 og altså længe før spørgsmålet var på dagsordenen.

Afslutningsvis gør Berlin sig atter til fortaler for negativ frihed og igen med et hint til demokrati:

> *"Pluralism, with the measure of 'negative' liberty that it entails, seem to me a truer and more humane ideal than the goals of those who seek in the great disciplined, authoritarian structure the ideal of 'positive' self-mastery by classes, or peoples, or the whole mankind. It is truer, because it does, at least, recognize the fact that human goals are many, not all of them commensurable, an in perpetual rivalry with one another (...) To say that in some ultimate, all-reconciling, yet realizable synthesis duty* is *interest, or individual freedom* is *pure democracy or an authoritarian State, is to throw a metaphysical blanket over either self-deceit or deliberate hypocrisy*"[10].

Der er således ifølge Berlin ikke tale om 'den rene vare', men netop en blanding med lidt fra begge sider af frihedsbegrebet – dog med størst vægt på negativ frihed – da målene netop er mangfoldige og ofte usammenlignelige, hvorfor de ikke bør begrænses alene til et autoritært, 'positivt' frihedsideal. Men han finder også, at det er fejlagtigt, at frihedsbegrebet er lig med det rene demokrati.

Spørgsmålet er imidlertid, hvorvidt Berlins definition er tilstrækkelig dækkende?

For bred definition

For hans definition af frihedsbegrebet er så bred, at den ikke er helt dækkende, når det gælder en nærmere beskrivelse af retten til privatliv og hermed sikring af ens personlige data. Eksempelvis er det begrænset, hvad der kan lægges i formuleringen, der går igen i begge frihedsbegreber om at "to do or be". Hvad er det, man kan være eller gøre? Er "to be" således at have friheden til at være en privatperson i juridisk og politisk forstand, der som sådan skal respekteres af myndighederne? Det fremgår ikke tydeligt af teksten og er for en stor dels vedkommende op til fortolkning. Ej heller tydeliggøres det, hvad der menes med "the source of control or interference". Er det staten? Kan det også være private firmaer eller individer? Igen med det forbehold af essayets datering, må det siges,

[8] Ibid: 24
[9] Ibid: 30
[10] Ibid: p. 31

at det ikke er brugbart i forbindelse med indsamling, oplagring, brug eller misbrug af personlige oplysninger. Det kan stort set udlægges efter eget ønske *eller* er til en vis grad indholdsmæssig tømt for mening.

Ud over det to-delte begreb vil jeg kort kommentere Berlins status-begreb. Ligger der i det at blive 'genkendt' og blive opfattet som en 'responsible agent', at man er respekteret, har ret til et privatliv og at myndighederne ikke kan træde over den grænse, der er gældende for den personlige sfære? Her mener jeg atter, at spørgsmålet er åbent for fortolkning, idet Berlin ikke siger noget særligt præcist i den retning. Igen – selv om han skrev dette lang tid før Big data, er det dog tydeligt at han navigerer imod totalitære styrer. Og disse gjorde jo en stor dyd ud af at indsamle privat og personlig information gennem de forhåndenværende teknologier. I hvert fald bør meningen nok tydeliggøres. Hans demokratiopfattelse er jeg derimod enig i og vil derfor ikke diskutere denne nærmere.

Berlins holdninger er heller ikke gået upåagtet hen og har mødt kritik fra flere sider; en kritik som jeg dog vil forbigå i denne sammenhæng. Når jeg i det følgende alligevel anvender Berlins definitioner, er det fordi jeg finder, at det trods alt er de bedst dækkende, når man skal beskæftige sig med frihedsbegrebet. Som sagt kan de dog ikke stå alene, men fordrer en uddybning. Til dette vil jeg se nærmere på Ronald Dworkins kritik af antiterrorlovgivningen. Men først en kort 'introduktion' i form af George W. Bush's tale få dage efter terrorangrebet mod World Trade Center i New York**.** Talen er relevant i denne sammenhæng, da den indvarsler dels den følgende antiterrorlovgivning og de deraf følgende politiske tilstande, dels begrunder og fortolker Bush netop terrorangrebet i lyset af frihedsbegrebet.

Bush's tale

I en retorisk flot stil indvarslede præsident Georg W. Bush i sin tale[11] på Capitol kun ni dage efter 9/11, hvad der var i vente i terrorbekæmpelsens navn. Et af citaterne er dette manikæiske: *"This is the world's fight. This is civilization's fight. This is the fight of all who believe in progress and pluralism, tolerance and freedom"*[12].

Senere i talen bebudede Bush også øget sikkerhed på flere planer, hvorefter han igen vender tilbage til friheden:

> *"Freedom and fear are at war. The advance of human freedom – the great achievement of our time, and the great hope for every time – now depend on us. Our nation – this generation – will lift dark treat of violence from our people and our future. We will rally the world to this cause by our efforts, by our courage. We will not tire, we*

[11] Address to a Joint Session of Congress and the American People, 20.9.2001, http://www.whitehouse.gov/news/releases/2001/09/print/20010920-8.html
[12] Ibid:3

> *will not falter, and we will not fail (…) I will not yield; I will not rest; I will not relent in waging this struggle for freedom and security for the American people"*[13].

Frihed er ifølge Bush noget, der kan sidestilles med andre goder som bl.a. sikkerhed, der skal forsvares – og altså lidt i tråd med Berlins. Men han postulerer også, at det er friheden, der er truet. Ikke desto mindre var de tiltag, hans administration tog for at sikre denne frihed, ironisk nok netop med til at formindsket selvsamme frihed. Og den efterfølgende anti-terrorlovgivning er endvidere gået terroristernes ærinde; nemlig ved at begrænse befolkningens demokratiske rettigheder. Det sidste følger Dworkin op på.

Frihed kontra sikkerhed

Forudsætningen for at forstå de indgreb i vor frihed og hermed problemet med personfølsomme oplysninger er, som nævnt, at se på følgerne af antiterrorlovgivningen efter 9/11. Uanset hvor frygtelig angrebet på de to tårne var i New York, sætter Dworkin det i perspektiv ved at opregne, at mens al-Qaeda (kun) dræbte ca. 3.000 mennesker ved angrebet, svarer det til en fjerdedel af antal myrdede i hele landet i 1999. Han beskæftiger sig i artiklen med sammenhænge mellem frihed og sikkerhed i lyset af terrorisme. Mit udgangspunkt vil være hans essay *'The Threat to Patriotism'*. Heri forholder han sig meget kritisk til begivenhederne efter terrorangrebet i New York, hvor den amerikanske regering

> *"enacted legislation, adopted policies, and threatened procedures that are not consistent with our established laws and values and would have been unthinkable before"*[14].

Han henviser bl.a. til USA Patriot Act, der har en "*new, breathtaking vague and broad definition of terroism and of aiding terrorist"*[15]. Blandt meget andet giver loven ret til at gennemsøge privat bopæl, der tilhører både borger og udlændinge uden ejerens viden, hemmelig aflytning og begrænset eller forment ret til at en mistænkt kan vælge sin egen advokat. Dworkin kommer også ind på reaktionerne, der fulgte med terrorangrebet.

'Terrorising' eller 'terrifying'?

For antiterrorlovgivningen har mødt "*surprisingly little protest in America"*[16]. Det tilskriver Dworkin delvist den almene opfattelse af terroristerne som onde, kraftfulde, fantasifulde, med

[13] Ibid:5
[14] Ronald Dworkin, 2002: The Treat to Patriotism, New York Review of Books: 1
[15] Ibid:1
[16] Ibid:3

veltrænede og selvmordsfanatikere til rådighed. Men også: *"People's respect for human and civil rights is very often fragile when they are frightened, and Americans are very frightened"*[17].

Her blot ganske kort: Det er det nok nødvendigt at skelne mellem to engelske udtryk: *'terrorising'* og *'terrifying'*. For hvad var (og er) det, der ramte den amerikanske befolkning? Var det frygten for terror, for at blive terroriseret? Eller så at sige frygten for frygten? Jeg mener, at Dworkin mht. det sidste har fat i noget rigtigt, nemlig 'terrifying'.

I forbindelse med terrorismen henviser Dworkin til heksejagten i McCarthy-areaen "*among the worst stains of the record"*[18]og opfordrer til at amerikanerne i fremtiden må være mere varsomme. Bl.a. fordi det kan føre til en glidebane, hvor andre og mindre lovovertrædelser bedømmes hårdere end hidtil. Modargumentet, som bl.a. er fremført af dommer Jackson, er, at forfatningen og anstændighedsfølelsen ikke skal blive en 'selvmordspagt'. Men hvad vejer tungest – frihed eller sikkerhed?

Det ene på bekostning af det andet

Når det drejer sig om balancen mellem sikkerhed og frihed, mener mange, at det ene kan ske på bekostning af det andet. Men det er forkert, mener Dworkin:

> *"They suggest that "we" – Americans in general – must decide what mixture of security and personal freedom we want for ourselves (…) None of the administration's decisions and proposals will affect more than a tiny number of American citizens: almost none of us will be indefinitely detained for minor violations or offenses, or have our houses searched without our knowledge, or find ourselves brought before military tribunals on grave charges carrying the death penalty. Most of us pay almost nothing in personal freedom when such measures are used against those the President suspects of terrorism"*[19].

Det er klart, at meget få amerikanere risikerer at skulle stå for en militærdomstol eller er truet af dødsstraf (af denne grund). Men Dworkin tager fejl, når han i denne sammenhæng ikke ser truslen mod friheden. Med lovgivningen er mulighederne legio for myndighederne til at gribe ind i borgernes frihed – netop med henvisning til deres og nationens sikkerhed. Og i denne sammenhæng nævner Dworkin slet ikke borgernes data-sikkerhed.

Det gør han til gengæld et andet sted. I *'Terror & the Attack on Civil Liberties'* skriver han: "*The administration has greatly expanded both surveillance of private individuals and the collection of data about them"*[20].

[17] Ibid:3
[18] Ibid:4
[19] Ibid:7
[20] Ronald Dworkin, 2003: Terror & the Attack on Civil Liberties', set på nettet 24,2.2014:1

Og så kommer han ikke yderligere ind på emnet. I øvrigt mener han, at faren ved terrorismen er "*self-inflicted*"[21], idet Bush-regeringens svar på faren har *"ignored or violated many fundamental individual rights and liberties, and we must now worry that the character of our society will change for the worse"*[22].

Kritikken i USA er gået på, at politikerne ikke er i overensstemmelse med forfatningen, krænker borgernes fundamentale menneskerettigheder og er i modstrid med internationale love. Dworkin finder endog lovgivningen umoralsk.

I det følgende vil jeg se nærmere på Dworkins frihedsbegreb.

Frihed og lighed

Selve frihedsbegrebet definerer Dworkin i *'The Place of Liberty'* som negativ frihed[23] – *"freedom from legal constraint – not freedom or power more generally"*[24]. Men han er i denne sammenhæng ikke som sådan interesseret i frihedsbegrebet, men kun som forbindelsen mellem frihed og fordelt lighed; som et aspekt ved lighed *"rather than, as it is often thought to be, an independent political ideal potentially in conflict with it"*[25].

Dworkin advarer mod dogmatisme, der gør vores opfattelse af frihed til en fundamental værdi, der ikke må ofres for lighed. Og det hedder videre, at de dominerende, politiske opfattelser af frihed ikke er nogen licens, men et sæt *"of discrete rights to particular freedoms"*[26]. For ham kan frihed og lighed ikke komme i konflikt som to fundamentale politiske værdier,

> *"because equality cannot even be defined except by assuming liberty in place, and cannot be improved, even in the real world, by policies that compromise the value of liberty (..) if the two virtues do conflict, equality must have priority"*[27].

Hermed mener han, at nok skal de to begreber – frihed og lighed – ses i en sammenhæng og er forudsætninger for hinanden, men i enhver grundlæggende konkurrence mellem dem vil friheden altid tabe.

Selv om jeg ikke har medtaget alle Dworkins mellemregninger, men koncentreret mig om udsagnet, kan man så være enig i, at lighed (altid) har højere prioritet end frihed? Tager vi det for pålydende, holder hans argumentation så? Skønt lighed er et smukt begreb, mener jeg ikke, at hans argument er dækkende. For med hans negative frihedsbegreb skulle netop friheden være altafgørende og have en

[21] Ibid:1
[22] Ibid:1
[23] Ronald Dworkin, 2000: The Place of Liberty, ch. 3 in Sovereign Virtue. The Theory and Practice of Equality:120
[24] Ibid:120
[25] Ibid:121
[26] Ibid: 127
[27] Ibid: 182

højere prioritet end noget andet. Selv mener han altså det modsatte, derfor vil jeg lade det blive ved det og vende tilbage til følgevirkningerne af 9/11.

En glidebane

For med Dworkins friheds/lighedsbegreb har vi fjernet os fra terrorismen og dens følgevirkninger. Det vil jeg nu vende tilbage til med Lucia Zedners artikel[28], der dog lægger vægten på de kriminalistiske aspekter ved terrorlovgivningen. Heri skriver hun, at den internationale anti-terrorkamp "*poses no small threat to the very liberties it purports to protect"*[29]. Hun henviser til P. Thomas (2003), der konkluderer, at "*the idea of trading off freedom for safety on a sliding scale is a scientific chimera (…) Balance should not enter equation: it is false and misleading"*[30].

Zedner finder, at talen om balance er en politisk farlig metafor: *"Claims to rebalance in 'public interest' or 'national security' are laid down as trump cards against which any individual claim to liberty cannot compete"*[31].

I stedet er der behov for, at der formuleres en fælles interesse i at beskytte civile friheder mod kravet om sikkerhed. Når det hedder sig, at 'folk som os' ikke har noget at frygte pga. sikkerhedsmål, må dette være "*born of naive failure of imagination"*[32]. For, som hun skriver, vi skal ikke undervurdere i hvilket omfang disse sikkerhedsmål underminerer almindelige borgeres frihed i form af elektronisk overvågning, undersøgelse af såvel deres person som ejendom, identitetstjek osv.

Det gennemgående i hele hendes artikel er, at også hun ser faren ved at kravet om sikkerhed overtrumfer frihedsrettigheder og den enkeltes frihed. Men også at det er en alvorlig fejltagelse at tro, at dette ikke vedrører os, som 'almindelige' mennesker – heri ligger indirekte en kritik af Dworkins synspunkt. Der kunne siges meget mere om hendes interessante artikel, som jeg er enig i, men her bliver jeg desværre nødt til at fatte mig i korthed og vil i det følgende se nærmere på, hvad der menes med begrebet 'privat'.

'Privacy'

I hele det foregående har jeg især koncentreret mig om det negative frihedsbegreb. Heri indgår som et naturligt led det engelske ord '*privacy',* der kan oversættes med såvel 'privat' som 'privatliv'. Jeroen van den Hoven definerer det som bestående af behov, ret og et aspekt ved menneskelig vær-

[28] Lucia Zedner, 2005: Securing Liberty in the Face of Terror: Reflections from Criminal Justice.
[29] Ibid:507
[30] Ibid: 510
[31] Ibid: 513
[32] Ibid: 515

dighed – selv om udtrykket ifølge Wagner DeCew (1997) er ”*vague, fuzzy, and hard to explicate or pin down”*[33]. I det følgende vil jeg bruge samlebetegnelsen privacy.

Den offentlige debat har ifølge ham i dette århundrede stort set drejet sig om tre positioner:

- Vi skal ikke bekymre os om privacy, da alle pga. den store informationsmængde kan vide alt om alle, hvorfor det er absurd at forsøge at kontrollere det.
- Et vestligt demokrati ikke har råd til et højt niveau af individuel privacy. Selv om det var muligt, er det ikke ønskeligt.
- Og der er gode moralske grunde til at beskytte den enkelte mod Big Brother, data-grådige selskaber og medborgere, der snuser omkring.

De to første punkter er jeg langt fra enig i. Tværtimod mener jeg, at der er endog mange grunde til at vi bekymrer os (dette vil blive uddybet senere), ligesom jeg ikke finder synspunktet, om at vi ikke har råd til, endsige at det ikke skulle være ønskeligt, at beskytte den enkeltes privacy, for korrekt (begrundelse herfor ligeledes senere). Det tredje punkt dækker derimod min opfattelse helt.

Van den Hoven vil dog ikke gå nærmere ind i en definition af privacy, men vil derimod se på, hvilke grunde regeringer og ikke-regeringer har for at indsamle informationer om enkeltindivider. Og her skelner han mellem dem, der har interesser i, hvad han kalder data-subjektet og dem, der ikke har.

Det fører igen til fire former for data-indsamling:

- Regeringer ønsker at bruge data til at yde en bedre service – i denne forbindelse henviser han bl.a. til de skandinaviske lande.
- Kommercielle selskabers ønske om ligeledes at yde deres kunder eller klienter en bedre service.
- Selvsamme selskaber kan have finansielle grunde til at indsamle data om deres kunder, partnere og ansatte
- Og endelig har regeringer interesse i at sikre den rette fordeling af *public goods.*

Det er for så vidt udmærket, men intet af dette omfatter dog det misbrug, der kan ske af såvel regeringer som kommercielle selskaber, hvilket jo er emnet for denne opgave. Derfor vil jeg i det følgende afsnit henvise til Dahls begreb om personlig autonomi.

[33] Jeroen van den Hoven (ed), 2014: Information Technology, Privacy, and the Protection of Personal Data:302

Personlig autonomi

Robert A. Dahl beskriver demokrati som folkets styre ud fra den antagelse, at almindelige mennesker sædvanligvis er kvalificeret til at regere sig selv. Dette uddyber han med sin antagelse om *personlig autonomi*, som han kalder en 'forsigtighedsregel: *"In the absence of compelling showing to the contrary everyone should be assumed to be the best judge of his and her own interests"*[34].

Dahls begreb om personlig autonomi tilføjer på den ene side et lag mere til det negative frihedsbegreb samt til van den Hovens privacybegreb, og danner på den anden side for mig at se en tydelig overgang til den sidste del af mit teoretiske afsnit, nemlig en uddybning af begreberne om det private eller privatliv.

Intim-cirklen

En nærmere definition af privacybegrebet har jeg på nær van den Hoven imidlertid ikke fundet i den anvendte filosofi. Så i stedet har jeg søgt en uddybning i Lou Hodges udlægning i hendes kapitel *'Privacy and the Press'*[35]. Heri citerer hun Sissela Boks (1982) definition som "*the condition of being protected from unwanted access by others – either physical access, personal information, or attention"*[36].

Mens Alan Westing (1967) definerer det som en beslutning om, hvordan og i hvilken grad information om en selv er kommunikeret til andre.

En anden, hun henviser til, er A.C. Breckenridge (1980) med et længere citat, der også omhandler personlige informationer:

> *"Privacy, in my view, is the rightful claim of the individual to determine the extent to which he wishes to share of himself with others and his control over the time, place, and circumstances to communicate to others. It means his right to withdraw or to participate as he sees fit. It is also the individual's right to control dissemination of information about himself; it is his own personal possession"*[37].

Atter henviser Hodges til Westin, der kalder dette retten til at definere ens egen *intim-cirkel*. Dvs. alt det kun vi selv ved; vore fantasier, uartikulerede håb og minder, der vil blive invaderet og nærmest vanhelliget, hvis nogen fik viden om dette mod vor vilje.

Ovenstående kan opfattes som en ekskurs, men jeg mener, at det er vigtigt at få denne uddybning med for at forstå, dels hvad der kan rummes i det negative frihedsbegreb, dels hvori problemerne ligger i brug – og misbrug – af vore personfølsomme data, som er min case i det følgende.

---

[34] Robert A. Dahl, 1989: Democracy and its critics:100
[35] Lou Hodges, 2009: Privacy and the Press in Handbook of Mass Media Ethics
[36] Ibid: 277
[37] Ibid: 277

Big data

Big data er summen af de spor – den gigantiske mængde data – vi afsætter, når vi surfer på Internettet, skriver e-mails, sms'er, twitter, går på de sociale medier, googler, chatter, gør indkøb online, skyper, bruger bilernes GPS-systemer eller vores smartphones. Big data er derfor private. Helt personlige. Selvfølgelig er der også data, der udveksles mellem myndigheder eller som de sender til os. Men det interesserer ikke brugerne. For brugerne er *ikke* os. Det er oftest offentlige myndigheder, der fungerer som aktive aktører og/eller mellemmænd, kommercielle virksomheder samt mega-organisationer, der indsamler og misbruger vore data. Med dette misbrug bliver det enkelte individ, borgeren, transparent. Så vi har ikke længere frihed til at disponere over vore egne data. På denne måde sammenvæves negative og positiv frihed – vort krav om frihed til og frihed fra. Kampen for privatliv er blevet kaldt for det 21. århundredes borgerrettighedskamp. For vore data er således ikke længere private. I det følgende vil jeg give nogle eksempler på dette misbrug. Men først en lille omvej via *whistleblowers.*

Whistleblowers

Fra tidernes morgen har der givet eksisteret whistleblowers. I nyere tid skal blot nævnes Daniel Ellsberg (7.000 Pentagon-dokumenterne om krigen i Vietnam; i sidste ende frikendt), samt Julian Assange fra WikiLeaks (bl.a. 90.000 hemmelige NATO-dokumenter om USA's krigsførelse i Afghanistan; han lever nu i asyl), og *hacktivister* som Bradly Manning, (250.000 dokumenter fra amerikanske ambassader og 500.000 hærrapporter fra henholdsvis krigene i Afghanistan og Irak; en læk han blev idømt 35 års fængsel for). Hacktivister er *ikke* hackere, idet de vil fikse fejlene i teknologien hos bl.a. offentlige myndigheder og også ofte informere offentligheden. Vi har også haft vor hjemlige whistleblower i form af Frank Grevil (læk af hemmeligstemplede Irak-vurderinger; en læk, der kostede ham fire måneders fængsel).

Men for ganske almindelige mennesker har ingen næppe haft en tilsvarende betydning som Edward Snowden, som foreløbig er endt i Rusland. Med et udtal af læk på baggrund af titusinder udleverede dokumenter til en række vestlige aviser i 2013 har han påvist den amerikanske sikkerhedstjeneste, National Security Agency's, NSA's, massive dataovervågning. Denne har fundet sted både i USA og i resten af verden af såvel politikere, virksomheder som andre borgere – og det danske klimatopmøde COP 15 i 2009; det sidste har den danske regering imidlertid totalt afvist. For dækning af Snowdens lækage modtog *Washington Post* og *Guardian U.S.* i april 2014 årets Pulitzer Price for public service. NSA har et budget på 75 mio. dollar årligt [38], og de indsamlede oplysninger har beviseligt ført til miskreditering af politiske modstandere, journalister og borgerretsorganisationer [39]. De amerikanske myndigheder har således haft adgang på verdensplan gennem såkaldte 'bagdøre' og 'sikkerhedshuller' til personlige data fra bl.a. smartphones, Facebook, Gmail og Hotmail. Igen – størstedelen af de data, der indsamles, er vores.

[38] Information 19.5.2014
[39] Glenn Greenwald, 2014, Overvåget: 213

Vi taler derfor ikke længere om gigabyte men derimod enorme størrelser som petabytes (10^{15}) og exabytes (10^{18}), og i 2013 antog man, at verdens samlede informationslager udgjorde 1.200 exabytes [40].

For datamægden er så stor, at den ikke er menneskeligt muligt at overvåge. I stedet sker det ved hjælp af algoritmer – små programmer, der automatisk reagere på eksempelvis suspekt adfærd og derfor kan komme til at stemple dig som potentiel terrorist. Det kan igen føre til uretmæssig afvisning, når man vil flyve eller ved indrejse i et andet land, og måske kigger også skattevæsenet med nu man har så mange data[41]. Andre overvågningsredskaber er, som Snowden påviste, NSA's program Prism, der er en såkaldt semantisk analyse, et statistisk computerprogram, der i stedet for at basere sig på genkendelige nøgleord (som f.eks. ordet 'bombe') gætter sig til meningen med en besked[42]. Hvis man har tilstrækkelig detaljeret viden om den enkelte telefons tidligere bevægelser, kan man forudsige dens fremtidige position time for time med op til 93 pct.s sikkerhed.

> "*Lige siden Aristoteles har vi kæmpet for at forstå årsagerne til alting. Men det er ved at ændre sig. Med Big data-tidsalderen kan vi bearbejde helt ufattelige mængder af information og data, der giver os uvurderlig indsigt i, hvordan ting hænger sammen – men ikke hvorfor de hænger sammen, som de gør*",

siger Viktor Meyer-Schönberger[43].

Terrorpakke I og II

Trods Grundlovens § 72 om boligens ukrænkelighed og privatlivets fred holder Danmark sig heller ikke tilbage. Ifølge *Information*[44] blev danskerne i 2013 registreret 3,5 billioner gange (10^{12}) på mobil eller internet. Det er mere end en gang i minuttet for hver enkelt borger døgnet rundt og en firedobling i forhold til året før. Denne indsamling og opbevaring sker på trods af, at en evalueringsrapport fra Justitsministeriet fra 2012 viste, at den store indsamling stort set er nytteløs, da hverken politiet eller PET bruger den i et særligt stort omfang. Faktisk har politiet kun anvendt disse data en gang i en sag om indbrud i en netbank, uden at det dog førte til opklaring af forbrydelsen. Det samme er tilfældet IUSA, hvor de terrorplaner, der er blevet forpurret, ikke er et resultat af NSA's overvågning, men alle er blevet løst gennem almindeligt politiarbejde

De mange registreringer af danskernes kommunikation skyldes den såkaldte *logningsbekendtgørelse*[45], der trådte i kraft som led af Terrorpakke II[46]. Men allerede i 2002 blev Terrorpakke I[47] indført. Den vedr. hvad dataovervågning angår især mobiltelefoni.

---

[40] Politiken 29.12.2013
[41] Information 4,-5.1.2014
[42] Politiken 9.8.2013
[43] Politiken 29.12.2013
[44] Information 9.1. og 17.3.2014
[45] Bekendtgørelse nr. 988 af 28. september 2006
[46] Lov nr. 542 af 8. juni 2006 (Terrorpakke II)
[47] Lov nr. 378 af 6. juni 2002 (terrorpakke I)

Men med Terrorpakke II blev der indført den såkaldte *sessionslogning*, der gik videre end det EU-logningsdirektiv, der dannede grundlag for Terrorpakke I. I bekendtgørelsen hedder det således i § 5, at udbyderne skal registrere afsender og modtagers internetprotokol-adresse, transportprotokol, afsenders portnummer og tidspunkt for kommunikationens start og afslutning. Endvidere skal udbyderne registrere den tildelte brugeridentitet, navn og adresse på abonnent eller internetbruger. Ligeledes skal det lokale netværks præcise geografiske eller fysiske placering samt identiteten på det benyttede kommunikationsudstyr opgives. Endelig skal afsendere og modtagers e-mail-adresser registreres.

Lovgivningen betyder således, at teleudbyderne skal gemme data i et år, om hvem den enkelte kunde sms'er og ringer til, vedkommendes trafik på nettet, og hvor personen befinder sig på det pågældende tidspunkt. Ifølge ovennævnte artikel fra *Information* betyder det, at myndighederne med dette krav kan kortlægge både sociale netværk og bevægelsesmønstre i en høj detaljeringsgrad. Mobiltelefonoplysninger gemte de fleste udbydere i forvejen, men som noget nyt skulle de for internetbrug registrere, hvem der får hvilke IP-adresser på hvilket tidspunkt, samt hvilke IP-adresser man forbinder til.

Denne sessionslogning medfører ikke blot udgifter på et tocifret millionbeløb hos udbyderne, det er også en registrering, der som nævnt går ud over EU-direktivet. I loven er der indsat en revisionsbestemmelse, men trods pres fra flere sider er en revision gentagne gange blevet udskudt med henvisning til en reform fra EU, som der dog aldrig blev sat tidsfrist på. Men Justitsministeriet bebudede, at lovforslag herom vil blive fremsat i efteråret 2014, hvis EU's revision af logningsdirektivet blev yderligere forsinket. Dog – her blev ministeriet overhalet indenom.

EU-direktiv ugyldigt

For pludseligt tog tingene fart. I *Morgenavisen Jyllands-Posten*[48] 8. april 2014 erklærede Forbrugerrådet Tænk, Rådet for Digital Sikkerhed og Ingeniørforeningen i fællesskab at indsamlingen af data og personlige oplysninger om danskerne er gået amok på nettet og at forbrugersikkerheden reelt er sat ud af kraft – et argument de senere har gentaget. De fandt det på høje tid, at den danske persondatalov strammes og gøres tidssvarende, da den er lavet inden cookies, sociale medier og Big data. For som seniorjurist Anette Høyrup, Forbrugerrådet Tænk, siger til avisen: "*Vi mister retten til at kontrollere vores oplysninger. Vi ved ikke, hvor de havner, og hvad de bliver brugt til i fremtiden"*.

Samme dag var *breaking news*, at EU-domstolen helt uventet erklærede EU's logningsdirektiv for ugyldigt. Direktivet kræver[49] bl.a., at teleselskaberne i medlemslandene gemmer oplysninger om alle borgeres opkald og sms'er, og hvilke telefonmaster de er koblet på, samt oplysninger i forbindel-

[48] Morgenavisen Jyllands-Posten 8.4.2014
[49] Information 9.4.2014

se med internetbrug. Oprindeligt var det tanken, at direktivet skulle harmonisere logningsregler i de enkelte medlemslande. Men sådan gik det ikke. Forfatningsdomstolene i både Tyskland og Rumænien har fundet direktivet forfatningsstridigt, og Sverige blev idømt en millionbøde for at nøle med indførelsen af direktivet.

EU-domstolens afgørelse skete efter henvendelse fra domstole i Østrig og Irland, og EU-domstolen giver følgende begrundelse, at direktivet[50]:

> *"i særlig alvorlig grad gør indgreb i den grundlæggende ret til respekt for privatliv og beskyttelse af personoplysninger, uden at dette indgreb er begrænset til det strengt nødvendige".*

Og senere i dommen hedder det:

> *"Domstolen fastslår endvidere, at direktivet ikke fastsætter tilstrækkelige garantier, der gør det muligt at sikre en effektiv beskyttelse af data mod misbrug samt ulovlig adgang til og benyttelse af data".*

Med henvisning til de oplysninger, som EU hidtil har gemt, hedder det i begrundelsen:

> *"Disse data kan samlet give meget præcise oplysninger om privatlivet hos de personer, hvis data er lagret, f.eks. indkøb af dagligvare, faste eller midlertidige opholdssteder, aktiviteter, sociale relationer og de sociale miljøer, de færdes i".*

EU-domstolens afgørelse er epokegørende, da det er en af de første gange, at EU's menneskerets-charter fra 2009 i praksis anvendes til at garantere retssikkerheden for unionens borgere.

Juraprofessor på Københavns Universitet, Peter Blume[51], opfordrer til, at den danske registrering sættes i bero, indtil der er en afklaring af, hvorvidt der sker tilstrækkelig beskyttelse af privatliv og personoplysninger. Det er dog i skrivende stund uvist, hvordan Justitsministeriet vil reagere på EU-domstolens afgørelse. De svenske teleselskaber *har* efter dommen stoppet logning.

Intentionen bag de danske terrorpakker var (og er) at opspore og forhindre grov kriminalitet, men først og fremmest at forebygge terror. Pakkerne fik bred opbakning i Folketinget, uagtet det begrænser vore, borgernes, frihedsrettigheder. Det skal dog tilføjes, at Big data kan også være anvendelige i ikke-voldelige sammenhænge som eksempelvis ved trafikplanlægning og sygdomsovervågning (selv om Google Flu Trend, der ud fra søgninger på nettet forsøger at forudsige en evt. influenzaepidemi, stadig skyder 30 pct. over målet på trods af, at algoritmerne er blevet ændret[52]), men og-

[50] Newz.dk og Computerworld.dk 8.4.2014
[51] Information 9.4.2014
[52] bits.blog.nytimes.com – set på nettet 24.4.2014

så for arbejdsgivere til at tjekke nuværende eller kommende medarbejdere, gøre nogle flybilletter dyrere, idet prisen indrettes efter vort søgningsmønster på nettet etc.

Terrorpakkerne er dog ikke det eneste indgreb fra myndighedernes side.

Et par danske eksempler

Tidligere hospitalspatienter i København kunne indtil slutningen af marts 2014 risikere at blive ringet op af et analyseinstitut i forbindelse med en bruger-tilfredsheds-undersøgelse. Instituttet var af hospitalsafdeling blevet forsynet med patientens navn, telefonnummer, indlæggelsesdato og oplysning om, hvilket hospital den pågældende havde været indlagt på. Det er nu stoppet efter flere protester fra patienterne. I øvrigt har ikke færre end 90.000 offentligt ansatte adgang til de elektroniske patientjournaler[53]. Dertil kommer de utallige eksempler på, at myndighederne har ladet personfølsomme oplysninger flyde på nettet – senest er det påvist at være tilfældet i 21 kommuner[54].

En dansk hacktivist har påpeget et sikkerhedsbrist hos teleselskaberne, der gjorde det muligt at udregne cpr-numre – bl.a. for et par hjemlige toppolitikere – alene ved hjælp af en persons fødselsdato og navn. Det blev han idømt en bøde på 3.500 kr. for i byretten[55].

Samme måned blev *Nets*, der udbyder bl.a. Dankortet, Betalingservice, NemID og e-boks, solgt for 17 mia. kr. til ATP og to amerikanske kapitalfonde. Mange spørgsmål har rejst sig i denne forbindelse – ikke mindst hvordan man i fremtiden vil sikre beskyttelsen af vore meget følsomme, økonomiske data. Men kort efter viste det sig, at det var så som så med sikkerheden.

SE & Hør-sagen

For det var ikke sidste gang *Nets* var i offentlighedens søgelys. Mandag den 28. april 2014 udkom bogen *'Livet, det forbandede'* af en tidligere journalist på ugebladet *Se & Hør*. Heri fremkom – i fiktionens form – oplysninger om, at en medarbejder i relation til *Nets* fra 2008 til 2012 mod betaling havde forsynet ugebladet med kreditkortoplysninger om 'de kendte og kongelige'. Oplysningerne, der gjorde det muligt at følge de pågældendes færden, er senere bekræftet af en række tidligere medarbejdere på bladet. Halvandet år forinden var *Nets* med dokumentation blevet advaret om sikkerhedshullet, dog uden at det førte til opklaring, endsige politianmeldelse; i tidligere episoder med snagende *Nets*-medarbejdere har dette kun ført til afskedigelser. Politianmeldelse kom med årets afsløring mod koncernen Aller Media, der ejer bladet. I hastigt tempo fulgte hjemsendelse af en række medarbejdere på *Ekstra Bladet, Billed Bladet* og *Se & Hør,* lige som ugebladets fhv. chefredaktør, Henrik Qvortrup, sagde sin stilling op på *TV2,* blev anholdt og sammen med to andre senere

[53] Radioavisen, DR, 12.5.2014
[54] P1, DR, 22.5.2014
[55] Information 16.4.2014

chefredaktører af bladet blev sigtet i sagen. Aller Fondens bestyrelsesformand, Linda Nielsen, er gået osv., osv. Det hele vil fortsætte længe efter denne opgave er afleveret.

Finanstilsynet har ikke været på kontrolbesøg på *Nets* i fire år, og Datatilsynet er ressourcemæssigt blevet syltet i adskillige år og skal reduceres yderligere[56] . Brud på datasikkerheden kan maksimalt koste en bøde på 25.000 kr., hvor f.eks. straframmen for forkert markedsføring går op til 2 mio. kr.

Justitsminister Karen Hækkerup krævede en redegørelse for mediesagen og bebudede en større undersøgelse af sikkerheden, lige som hun ikke vil udelukke ny lovgivning på området. En vel sen erkendelse og udtryk for både hykleri og dobbeltmoral al den stund regeringen som nævnt ikke har afkrævet sikkerhedsspørgsmålet større opmærksomhed, ej heller i forbindelse med Snowdens lækage om USA's overvågning af COP 15. Svaret herpå fra regeringens side var at "*vi ikke har grund til at tro, at der er foregået ulovlige efterretningsaktiviteter mod Danmark eller danske interesser*[57].

Se & Hør-sagen er blevet kaldt dansk presses største skandale, er et alvorligt brud på presseetikken og har givet anledning til selvransagelse i medierne. For nok er der tale om en grov kriminalsag, men ikke blot *Nets* men også det pågældende ugeblad har ulovligt og grænseoverskridende krænket privatlivets fred ved brug af personfølsomme oplysninger. Historien er atter et bevis på, hvor sårbare vore data er på nettet. At situationen ikke er enestående viser en tilsvarende sag fra Norge, hvor en bankansat ligeledes forsynede et ugeblad med kreditoplysninger, og ikke mindst skandalen med mobiltelefonaflytningerne foretaget af det Rupert Murdoch-ejede og nu lukkede, britiske *News of the World*, der var en af verdens største aviser.

Nu anvendte *Se & Hør* oplysningerne til ren sladder. Et mere uhyggeligt scenarie kunne være, hvis sådanne meget private oplysninger faldt i hænderne på eksempelvis kriminelle, personer blev udsat for identitetstyveri mv. En politimand var 7.000 gange inde i kriminalregisteret, før han blev opdaget. Hvorfor? Lignende eksempler er opstået i kørekortregisteret og CPR-registeret[58]. Men uanset hvilke lyssky hensigter, der måtte være, er det hver eneste gang misbrug af vore data, der finder sted.

Flere myndighedsindgreb

Regeringen vil med en ny lov styrke sikkerheden mod hackerangreb og anden it-kriminalitet[59]. Disse oplysninger skal samles i Center for Cybersikkerhed, der hører under Forsvarets Efterretningstjeneste (FE). Men ifølge lovudkastet er der ikke lagt op til en videreførelse af den hidtidige begrænsning, hvorved der ikke sker nogen behandling af krypterede data eller bliver gjort forsøg på at dekryptere dem. Ydermere kan FE opbevare data i 13 måneder, mens grænsen i dag er 14 dage. Det er med til at øge risikoen for misbrug. Sker der ikke ændringer i lovforslaget, er der frygt for, at FE får

[56] Debatten, DR, 6.5.2014
[57] Information 30.4.2014
[58] Debatten, DR, 6.5.2014
[59] Information 7.3.2014

mulighed for adgang til oplysninger over internettet, uden at det bliver muligt at følge med i, hvad FE gør med oplysningerne, og hvilke udenlandske tjenester, FE vælger at dele oplysningerne med. Og det sker allerede: Alene i Danmark har NSA i samarbejde med lokale efterretningstjeneste (sandsynligvis FE) indsamlet 23 mio. metadata i en 30 dages periode[60].

De praktiserende læger vil ifølge en lov fra 2013 fremover være forpligtet til at registrere og indberette oplysninger om kroniske patienter til en central database[61]. Dette sker uden patienternes informerede samtykke. De store datamængder, giver ifølge regeringens Vækstteam Danmark, mulighed for at tjene milliarder ved "*øget fokus på det kommercielle potentiale i anvendelse af data og systemer*". Således er lægemiddelindustrien interesseret i at købe adgang til anonymiserede dele af sundhedsregistret. Spørgsmålet er dog hver gang nye datamængder indsamles, om sikkerheden altid er sikret.

I det hele taget opfører statsmagten med dens offentlige myndigheder sig, som om det var dem, der er ejere af vore data.

Skulle der ske et positivt skift i de danske myndigheders holdning efter EU-dommen, er det ikke hermed givet, at kommercielle interesser så også ændres til det bedre. For som det vil være fremgået, er det ikke blot myndighederne, der gør brug af vore data i overvågningsøjemed, men også andre interesser er på spil; og ikke sjældent med hjælp fra det offentlige.

Databrokers

De grelleste eksempler på de såkaldte *databrokers* blev fremdraget af programmet *'60 minutes'* fra det amerikanske tv-netværk *CBS*[62], der blev vist på *DRK* i marts 2014. For i dag har de fem giganter Google, Facebook, Amazon, Apple og Microsoft men også andre private aktører adgang til ufattelige mængder af viden om, hvordan mennesker agerer på nettet.

I udsendelsen påviste værten Steve Kroft, at der er tale om en multimilliard dollar industri, der indsamler, analyserer og sælger personlige informationer om millioner af amerikanere. Om hvad de kan lide eller ikke-lide, deres vaner, nærmeste venner og daglige bevægelsesmønstre. Og oftest uden de pågældendes viden. Disse data er samlet med tilføjede navne. En af de største databrokers er Acxiom, der har i snit 1.500 stykvise informationer om mere end 200 millioner amerikanere.

Oplysningerne, der samles og sælges, omfatter eksempelvis religion, etnicitet, politisk tilhørsforhold, brugernavn, indkomst samt familiens sundhedsmæssige historie – herunder hvilken medicin, de bruger, hvem der lider af hvilke sygdomme, genetiske som psykiske, seksuel orientering, hvorvidt man er bøsse eller lesbisk, har alkohol- og spilleproblemer eller sidder i gæld, seksuelt overførte sygdomme og hvem der har købt sexlegetøj. Alene ud fra IP-adressen og pc'ens ID-nummer

[60] Information 13,5,2014
[61] Information 2.6.2013
[62] http://www.cbsnews.com/the-data-brokers-selling-your-personal-information, set på nettet 29.3.2014

kan databrokerne matche informationerne med andre online-genkendte. Det er der firmaer, som er specialiserede i. Med det populære og gratis spil Angry Birds, som millioner har downloaded til deres smartphones, kan firmaet bag følge enhver bevægelse hos brugerne og give oplysningerne videre til andre firmaer. Disse data fortæller, hvor man er, hvem man har besøgt, hvor man har købt ind, hvornår du forlader dit hjem eller arbejdsplads og hvornår du kommer tilbage. Systemerne søger også i folks private adresseliste på telefonerne.

Kun en enkelt databroker er blevet idømt en bøde på 800.000 dollars for vildledende handelspraksis, andre firmaer som Axciom, Epsilon og Experian obstruerer undersøgelser. Epsilon hævder i udsendelsen at have "*verdens største kooperative database med mere end 8 milliarder kundetransaktioner*". En af de mest kraftfulde lobbygrupper i Washington, Direct Marketing Association, har blandt sine kunder Google og Facebook, men – de sælger ikke deres informationer. De beholder dem for sig selv, som Kroft siger. Og her kan tilføjes: I kommercielt øjemed, idet data kan sikrer annoncekroner; penge som de stort set ikke betaler skat af, men gemmer i skattely. Eller de er yderst hjælpsomme og imødekommende overfor amerikanske myndigheder og NSA.

Dog har Microsoft appelleret en amerikansk dom, hvori det fastslås, at Microsoft skal ulevere alle e-maildata, der stammer også uden for USA, hvis der foreligger en amerikansk domstolsafgørelse herom.

Der eksisterer således ingen effektiv lovgivning, der sætter grænser for den kommercielle og myndighedernes udnyttelse af Big data. Og når dette kan ske i USA, er det intet, der forhindrer, at det også kan ske herhjemme. Vi ved det bare ikke…

Det er mange eksempler, der dog blot er udpluk, men når jeg har anvendt dem skyldes det, at jeg har fundet det nødvendigt for at anskueliggøre, hvor stort problemet med Big data er og hvor indgribende det er i vore frihedsrettigheder. Når *Information* fylder så relativt meget i referencerne - skyldes det, at avisen i sommeren 2013 bragte en større serie om data og siden har fulgt skandalerne tæt.

Også vort ansvar

Og til sidst: Computerspecialisten Jaron Lanier har foreslået en demokratisering, så vi ejer og kan handle med vore egne Big data. At vi bør kunne rette og slette vore data eller helt undgå registrering heraf – en nylig EU-dom giver retten til i 'visse sammenhænge' at blive 'glemt' i forhold til forældede eller forkerte oplysninger, Google linker til. Viktor Meyer-Schönberger har også en indirekte hilsen til Dahl, idet han finder behov for ændring af reglerne "*we use to govern ourselves*"[63]. Han taler direkte om nødvendigheden af et paradigmeskift, hvor vi skal bestemme, hvordan og af hvem, der skal besidde vore personlige informationer. Til det formål foreslår han et skifte fra individuelt samtykke til databrugernes

[63] Viktor Mayer-Schönberger og Kennet Cukier: Big Data, 2013:171

ansvarlighed. For som han skriver: ”*Big data erodes privacy and threatens freedom”*[64]. Og vi er med Luciano Floridis ord ikke blot forbruger men også producent af information[65].

Der findes også muligheder for at komme under myndighedernes radar og beskytte vore Big data ved kryptering i form af TOR, *The Onion Router*[66], eller ved at lægge sine data ’op i skyen’. Men det hjælper alt sammen ikke noget, så længe ikke mindst offentlige myndigheder tiltvinger sig adgang til (og handler med) vore data. Og med de mange data vil glemsel være umulig. Dertil strør vi selv sorgløst brødkrummer efter os på nettet i form af cookies, oplyser også unødigt vort CPR-nummer og tillader at eksempelvis vore smartphones kan lokalisere os. Vi kan dog også, som digteren Ursula Andkjær Olsen udtrykker det i forbindelse med, hvorvidt Edward Snowden skal have asyl i Danmark, som foreslået af Enhedslisten og Uffe Elbæks fra partiet Alternativet:

> ”*Statslig overvågning er jo ikke det eneste problem, vi har; markedet er også en big brother/mother (som omsorgsfuldt giver skræddersyede ’netoplevelser’ just4you). Der er virkelig brug for noget brug-kondom-på-nettet-oplysning. Det var en opgave, som staten burde påtage sig – måske ved staten bare heller ikke, hvordan man skal beskytte sig…”*[67].

Konklusion

Spørgsmålet om datasikkerhed er langt fra nyt, men især Snowdens lækager har skabt større opmærksomhed i offentligheden om problemet. At jeg tilhører den forkætrede journalistiske stand, lader sig ikke fornægte med mine mange, praktiske eksempler. Alligevel har det været nødvendigt for mig – også på det praktiske plan – at påpege de alvorlige problemer, der ligger i manglende beskyttelse af den del af vort privatliv og hermed vor frihed, som er forbundet med vore elektroniske data. Et problem og en manglende beskyttelse, som jeg ikke har fundet, at filosofien i tilstrækkelig grad har været opmærksom på.

Da jeg løbende har forsøgt at konkludere på de enkelte afsnit og citater, vil jeg her kun kort vende tilbage til teorien. Jeg kan ikke gå ind for ubegrænset frihed i Berlins negativ forstand af begrebet. For noget sådant vil fører til rent anarki, som ikke kan rummes i et demokrati. Et demokrati forudsætter imidlertid, at det sikrer borgernes sikkerhed og i så vidt muligt omfang deres frihed. Og hverken frihed eller sikkerhed eksisterer med Big data under de nuværende forhold; forværret som situationen er med bl.a. anti-terrorlovgivningen efter 9/11.

Det har derfor været vigtigt for mig ud fra den anvendte teori og med de anførte eksempler at vise, især hvor langt denne frihed rækker – eller netop ikke rækker. Går vi det skridt længere end Berlins definitioner og når vore dage med ”war against terror” kan man med rette spørge, som Dworkin og

[64] Ibid:163
[65] Luciano Floridi, 2014, Information Ethics: Its Nature and Scope: 42
[66] Andy Greenberg, 2012: This Machine Kills Secrets. How WikiLeaks, Hacktivists and Cyperpunks Aim to Free the World’s Information
[67] Politiken 8.4.2014

Zedner gør, om ikke dataovervågningen går terroristernes ærinde, netop ved at knægte en del af vort demokrati og vore frihedsgrader? Det er der blandt politikerne langt fra konsensus om. Tværtimod synes hovedparten af (også vore hjemlige) politikere at være af den modsatte opfattelse og har øget overvågningen af deres egne befolkninger. Men som van Hoven udtrykker det: *"We need to repair our boat at sea"*[68].

Da Facebookgrundlæggeren Mark Zuckerberg blev spurgt, hvordan Facebook opbevarer sine data og sikrer brugerens privatliv, lød hans svar: "*Jeg forstår ikke spørgsmålet. De, som ikke har noget at skjule, har intet at frygte"*[69]. Det er det samme argument, vi igen og igen hører fra politikerne, når de afviser misbrug af vore personlige data. Under radaren ligger, som det er fremgået, også hele det kommercielle område, der stort set er ureguleret, hvad datamisbrug angår. Såvel dette som hele det politiske område kræver derfor øget opmærksomhed fra filosofiens side.

[68] Jeroen van den Hoven (ed), 2014:303
[69] Information 23.4.2014

Litteraturliste:

Isaiah Berlin,1969: Two Concepts of Liberty in Four Essays on Liberty, Oxford University Press,

Ronald Dworkin, 2002: The Treat to Patriotism, New York Review of Books,

Ronald Dworkin, 2000: The Place of Liberty, ch. 3 in Sovereign Virtue. The Theory and Practice of Equality, Harvard University Press,

Ronald Dworkin, 2003: Terror & the Attack on Civil Liberties, The New York Review of Books, set på nettet 24.2.2014

Lucia Zedner, 2005: Securing Liberty in the Face of Terror: Reflections from Criminal Justice, Journal of Law and Society, vol. 32, no. 4,

Jeroen van den Hoven, 2014: Information Technology, Privicy, and the Protection of Personal Data, Cambridge Books online, set på nettet 12.3 2014

Viktor Meyer-Schönberger og Kenneth Cukier, 2013: Big Data, A Revolution That Will Transform How We Live, Work and Think, John Murray,

Robert Dahl, 1989: Democracy and its critics, Yale University Press,

Lou Hodges, 2009: Privacy and the Press in The Handbook of Mass Media Ethics, 2009, (ed.) Lee Wilkins and Clifford G. Christians, Routledge, New York,

Measures of Press Freedom and Media Contributions to Development, 2011, (ed.) Monroe E. Price and Susan Abbott with Libby Morgan, Peter Lang New York,

Terrorism and International Justice, 2003, (ed.) James P. Sterpa, Oxford University Press,

Andy Greenberg, 2012: This Machine Kills Secrets. How WikiLeaks, Hacktivists and Cyperpunks Aim to Free the World's Information, Dutton,

Glenn Greenwald, 2014: Overvåget, en indsiderberetning om Edward Snowden, NSA og den amerikanske overvågningsstat, Informations Forlag,

Luciano Floridi, 2014: Information Ethics: Its Nature and Scope, in Information Technology and Moral Philosophy (eds.) Jeroen van Hoven and John Weckert, Cambridge Books Online,

Address to a Joint Session of Congress and the American People, 20.9.2001, http://www.whitehouse.gov/news/releases/2001/09/print/20010920-8.html