Overvågning

Kan persondataretten gøre nytte?

Af Peter Blume

Abstract

Artiklen tager sit udgangspunkt i en overvejelse af hvad privathed med hensyn til information dækker over. Dette er ikke fuldstændigt klart, men centrale værdier er relateret til den enkeltes mulighed for at udøve kontrol og adgangen til at have et privat område ("at være alene"). Privathed betragtes som en positiv værdi, men er generelt betinget af de samfundsmæssigt dominerende politiske værdier og er ligeledes i betydelig udstrækning påvirket af den foreliggende informationsteknologi. Privathed er ikke nogen konstant værdi og må ikke tages for givet. Nutidens samfund er overvågeligt, og den digitale teknologi har gjort individet sårbart og transparent. Internettet fremhæves som både en velsignelse og forbandelse. En specifik form for overvågning må forstås og vurderes under hensyntagen til dens formål, de anvendte midler, hvor den finder sted, og de overvågedes og den overvågendes karakteristika. I den digitale verden er datasikkerhed det primære middel til at forebygge og begrænse overvågning. Den enkelte person er afhængig af de former for datasikkerhed, som den dataansvarlige iværksætter, idet det anvendte sikkerhedsniveau ofte vil være betinget af hensynet til omkostninger. Det fremhæves særligt, at den dataansvarlige typisk ikke har noget egentligt kendskab til teknologien og derfor i praksis er afhængig af andre, der faktisk installere de forskellige former for sikkerhed, idet den dataansvarlige ligeledes må stole på eksterne databehandlere, som i mange tilfælde faktisk foretager persondatabehandlingen. På mange måde garanterer den dataansvarlige ikke datasikkerheden. Gældende og fremtidig persondataret diskuteres herefter, idet persondataretten er rettens primære bidrag til sikring af privathed i den digitale verden. Særligt fremhæves persondatarettens grundprincipper, herunder proportionalitet. Det iagttages generelt, at persondataretten kan gøre overvågningen mindre privatlivskrænkende og ligeledes mere transparent, men at denne retlige orden ikke kan hindre overvågningen, idet den i bedste fald kan begrænse overvågningens omfang. På denne baggrund omtales det forslag til persondataforordning, som Europa Kommissionen fremlagde januar 2012, og som forventes vedtaget i 2015 eller måske først i 2016. Forordningen vil erstatte det gældende databeskyttelsesdirektiv og ligeledes persondataloven. Hovedformålet er at øge harmoniseringen i EU, idet det herved anerkendes, at megen persondatabehandling har en international karakter. Det fremhæves, at den traditionelle reguleringsmodel bliver opretholdt således at reglerne er adresseret til den dataansvarlige, hvis regelrette adfærd danner grundlaget for databeskyttelsen. Selvom forordningen indeholder enkelte nye rettigheder medfører den således ikke nogen empowerment af den enkelte person. Som noget positivt betoner forordningen hensynet til datasikkerhed og indfører en fremtidsorienteret forståelse af datasikkerhed ikke mindst via principperne om privacy by

Peter Blume, Professor dr.jur
Det Juridiske Fakultet, Københavns Universitet
(Peter.Blume@jur.ku.dk)

design og privacy by default. Forordningen anerkender endvidere, at det faktiske databeskyttelsesniveau afhænger af den dataansvarlige og pålægger denne at have en lokal databehandlingsansvarlig, der skal sikre, at forordningens regler bliver overholdt. Denne model vil bl.a. styrke Datatilsynets muligheder for at varetage sin tilsynsopgave. Indførelse af regler om meddelelsespligt i de tilfælde, hvor et sikkerhedsbrud har fundet sted, er ligeledes et væsentligt skridt i den rigtige retning. Afslutningsvis konstateres, at moderne digital overvågning ofte gennemføres skjult for den enkelte person, men at den utvivlsomt reducerer privatheden. I det hele taget befinder privathed sig konstant i en udsat farezone i den digitale verden.

> "And the people bowed and prayed to the neon god they made….and whispered in the sounds of silence"[1]

Guden er ikke længere neon, men er blevet visuel, cyberspace og materialiseret i internettet. En ny form for tilværelse, der både er en velsignelse og en forbandelse. Menneskets muligheder for at være sig selv og have et privat område mødes med udfordringer, der bl.a. kendetegnes ved mange former for overvågning. Neonguden findes stadig, men den er ikke den øverste guddom, og på samme måde som tidligere har de få fokus på den nye Guds tvetydighed og hermed forbundne risici, men de mange er troende og føres let ind i den nye tilværelse og uanset mange advarsler er der også stor tavshed.

1. Privathed

Privatlivets fred, privathed, privacy, kært barn har mange navne, men det fælles træk er, at det ikke er muligt at opnå enighed om hvad barnet præcist er. Der er ikke en autoriseret definition og måske er det ikke så vigtigt at nå frem til en sådan[2]. Alle har en fornemmelse af hvad det er og at privatheden angår muligheden for at være i fred - the right to be let alone[3] - og muligheden for at kunne kontrollere om og på hvilken måde oplysninger om individet bliver brugt. Opfattelsen af hvad der er privat er ikke konstant, men er betinget af den aktuelle samfundstilstand og ikke mindst af de informationsteknologier, der skaber mulighed for at andre kan observere og trænge ind i en persons adfærd. Privathed er på mange måder en flygtig størrelse, og det er ofte lettere at beskrive hvornår en tilstand ikke er privat end hvornår den er det.

Vanskelighederne med at indkredse og definere den ideelle privatlivstilstand er især karakteristisk for det psykiske privatliv, og gør sig i betydelig mindre udstrækning gældende i forhold til det fysiske privatliv, som hovedsageligt kun inddrages indirekte i det følgende. I almindelighed kan fremhæves, at hjemmet er hovedbastionen for begge former for privathed, selvom hjemmet ikke længere er omgivet af så faste mure og derfor i stadig stigende omfang har svært ved at værne især det informationelle privatliv.

I mange samfund, herunder hos os, betragtes privathed i hvert fald overordnet som en positiv værdi. Selvom årsagen hertil som nævnt ikke lader sig præcisere fuldt ud skyldes denne opfattelse, at den omstændighed, at den enkelte person har et beskyttet frirum, hvor personen kan være sig selv, og muligheden for at udøve kontrol med oplysninger om sig selv, har en betydelig appel i et samfund, der fremtræder som systemorienteret og især som uoverskueligt og dermed truende. Alan Westin[4] har fremhævet fire privatlivstilstande, som mange vil genkende som ønskværdige. Disse er "solitude", hvor personen kan være alene, "intimacy", der knytter sig til nære relationer med andre mennesker, "anonymity", der angår muligheden for ikke at blive overvåget", og "reserve", der fremhæver muligheden for at have mental fred eller distance. Uanset om man finder disse kodeord dækkende eller udtømmende er der ikke tvivl om, at privathed knytter an til fundamentale træk ved menneskelig tilværelse og dermed har en positiv status.

Dette er dog ikke naturgivent. Privathed sætter fokus på det enkelte menneske og er en liberalistisk værdi. Historisk har privathed ikke altid været anerkendt, idet dette forudsætter en bestemt samfundsmæssig styreform, der ikke sætter statens, det kollektives, interesse som den dominerende værdi således at det enkelte individs autonomi og identitet underordnes og udviskes af den interesse, som repræsenteres af det kollektive, der refererer til idealet om alle personers fælles velfærd (det kommunistiske samfund[5]). Behovet for informationelt privathed er endvidere betinget af leveomstændighederne og det teknologiske niveau. Mennesket skal have mulighed for at være sig selv og samtidig bliver privathed en ønskelig tilstand som følge af, at der udvikles teknologier, nok startende med bogtrykket, som gør det muligt at eksponere mennesket og dermed true det private område. Behovet for og interessen i det private har

dermed været stigende i takt med samfundsudviklingen og introduktionen af nye teknologier. Blandt de grundlæggende rettigheder, der fungerer som centrale værdier i demokratiske samfund, har privathed på denne baggrund fået øget betydning i dagens samfund.

Det er en velkendt og generelt anerkendt iagttagelse, at privatheden er udsat for mange trusler og udfordringer i nutidens digitaliserede samfund, hvor en risiko for underminering er nærværende. Den moderne informationsteknologi har ført til mange fremskridt for den måde mennesker lever på, men teknologien har også skyggesider, og i øvrigt er vi ikke nødvendigvis lykkeligere end vi var før den kom til. Teknologien indebærer en generelt højere transparens og den er i en vis forstand en fjende, der nedbryder de barrierer, som skal sikre den enkeltes privathed. Trangen, behovet, nødvendigheden, for at dele information, for at være sammen ("connectivity") uanset hvor vi er[6], sætter det private under pres. De sociale medier betoner det sociale, fællesskabet, som en kult, hvor tilbøjeligheden til ekshibitionisme lokkes frem[7]. Vi kan komme til at lide af FOMO ("fear of missing out"), hvor vi hele tiden søger os selv ved at søge de andre. Vi ved måske godt, at denne vej indebærer farer, men vi bevæger os stille og roligt ud ad den.

Det er ikke kun os selv, der understøtter dette pres, idet dette pres også beror på ydre trusler. Presset illustreres af de forskellige former for overvågning, som nutidens mennesker bliver og kan blive udsat for. Privathedens tilstand og dens modstandskraft kan på denne baggrund forstås ved et fokus på den trussel, som overvågningen repræsenterer, og herudfra kan der ydes et bidrag til at tilfredsstille det påtrængende behov for at forstå og indkredse den måde privatheden i det nutidige samfund kan beskyttes på.

2. Det overvågelige samfund

Overvågning i dens mange forskellige udtryksformer er blevet et stadigt mere fremtrædende fænomen og overvågningen har mere end så mange andre trusler offentlighedens bevågenhed, selvom denne opmærksomhed er flygtig og tit betinget af enkeltstående begivenheder. Et fokus på overvågning kan klargøre eller i hvert fald bidrage til at forstå den status privatheden har som værdi på det samfundsmæssige og det personlige niveau.

Det er efterhånden almindeligt anerkendt, at vi lever i et overvågeligt samfund, hvor der med udnyttelse af de muligheder den moderne teknologi har skabt i stigende omfang bliver foretaget overvågning. Det er ikke kun de kendte eller interessante personer, der bliver overvåget, men enhver person kan blive overvåget og stadig mere bliver alle overvåget med henblik på varierende formål. Overvågning er et livsvilkår i det nutidige samfund og det er den pris, som vi betaler for at nyde de goder, som den moderne informationsteknologi har ført med sig. Retligt kan prisens størrelse søges reguleret, men det er utopisk at forestille sig, at retten eller andre instrumenter kan fjerne overvågning og dermed ej heller den negative oplevelse af, at overvågningen finder sted. Overvågning er dog langt fra altid et onde, men i øget grad er den teknologiens skyggeside, og bortset fra de tidspunkter, hvor offentligheden bliver udfordret er det en skyggeside, som i realiteten bliver accepteret. Vi lever med det. Den megen opmærksomhed omkring overvågning har ikke medført en maskinstorm vendt imod teknologien eller en bevægelse, der vil føre samfundet tilbage til den tid, der ligger før digitaliseringen. Der er ikke i denne sammenhæng nogen tilbage til naturen strømning.

Vi opgiver ikke internettet og dets goder. Vi er fanget i nettet, og vi kan ikke slippe ud således som det illustreres af pligten til at have en digital postkasse[8]. Det ses som nødvendigt at acceptere, at samfundet er blevet transparent og de enkelte personer lever med at være synlige om end ikke alle vil være med i denne form for fællesskab. Anonymitet er blevet en stadig mere vanskelig opnåelig tilstand selv for den person, der vil være alene. Eksempelvis betaler de fleste med kreditkort frem for med de anonyme kontanter også i situationer, hvor dette ikke er særligt nødvendigt. Der endda en bevægelse i lovgivningen, som vil gøre det muligt ikke at modtage kontanter ved salg af bestemte serviceydelser eller varer[9]. Transparensen bliver stadig øget og samtidig er vi ikke gode til at beskytte os selv eller også accepterer vi blot, at dette nu engang er tingenes tilstand og en pris, der må betales med den risiko, at den en dag slet ikke opleves som en pris.

På denne bagrund er et nærliggende spørgsmål om der er noget at være bange for og om overvågning er noget farligt. Spørgsmålet er yderligere om der reelt er noget at gøre ved det og om overvågningen kan stoppes eller i hvert fald begrænses uden at teknolo-

giens fordele bliver sat over styr. Dette er temaet for de kommende betragtninger, der først sætter fokus på hvad overvågning egentlig er og dernæst på om persondataretten både i sin nuværende form og som den er udformet i forslaget til EU persondataforordning kan være et middel til at begrænse overvågningen. Databeskyttelse er en grundlæggende værdi, men spørgsmålet er om dette er mere end ord på papir.

Afslutningsvis knyttes tråden tilbage til databeskyttelsens sammenhæng med privathed. Som det fremhæves i betragtning 10 i præamblen til databeskyttelsesdirektivet (95/46 EF) udspringer databeskyttelse af værnet af privatlivets fred som fastlagt i Den europæsiske Menneskeretskonventions artikel 8, og der er en nær sammenhæng mellem de to former for grundrettighedsværn, idet et udgangspunkt i forhold til informationsteknologien ifølge betragtning 2 er, at "databehandlingssystemer er til for menneskets skyld". Databeskyttelse er dog mere end blot en del af privatlivets fred, jfr. også nedenfor under 5, idet denne beskyttelse er anerkendt som en selvstændig grundrettighed. Selvom overvågning kan være privatlivskrænkende begrunder dette, at der i det følgende særligt er fokus på persondataretten, som mest målrettet søger at inddæmme og regulere overvågningen.

3. Overvågning

Det er naturligt for mennesker at iagttage andre menneskers adfærd. Mennesket er et nysgerrigt dyr. Disse iagttagelser kan finde sted på sammenfaldende niveau og uden at være del af en hierarkisk relation mellem aktørerne. Denne såkaldte undervågning udgør ikke en væsentlig trussel for privatheden, selvom teknologien har gjort den mere udpræget og nærværende. Iagttagelser kan også tage sigte på udøvelse af kontrol eller indsamling af oplysninger til brug for forskellige formål, der er mere eller mindre ubekendte og ligeledes uønskelige for den iagttagede person. Dette er overvågning og bestemte typer af denne er problematiske i forhold til den personlige integritet og privathed. Ved vurderingen af om overvågning under dette perspektiv skal betragtes som negativt må en række forskellige momenter tages i betragtning[10].

3.1 Formål

Først og fremmest er overvågningens formål eller med andre ord hvad overvågningen skal bruges til væsentligt. Det er i vidt omfang formålet, der viser om overvågningen er fjendtlig eller venlig i forhold til den enkeltes privathed. Der findes naturligvis et utal af varianter, men det kan være nyttigt at skelne mellem om overvågningen tager sigte på offentlige eller private, herunder kommercielle, formål. Det kan i denne forbindelse have betydning at inddrage i hvis interesse overvågningen foretages, herunder i hvilken udstrækning denne interesse er samfundsmæssigt velbegrundet. Det kan endvidere tillægges betydning om overvågningsformålet er orienteret imod bestemte personer eller en større ubestemt kreds, idet sidstnævnte har den primære interesse for en forståelse af overvågningens natur. Overvågningen kan være i de pågældende personers interesse og f.eks. være en velfærdsforanstaltning (eksempel: overvågning af butik for at hindre røveri). Vurderingen af formålet må i almindelighed ske specifikt i forhold til den enkelte overvågning, jfr. yderligere hertil nedenfor.

3.2 Midler

Det er ikke udelukkende overvågningens formål, der må tillægges betydning. Det kan tillægges vægt i hvilken udstrækning de anvendte midler i sig selv er krænkende ved at komme for tæt på personen og det private område. I denne sammenhæng er det ikke nødvendigvis den moderne teknologi, der er i centrum. På en måde er den teknologisk baserede overvågning venlig i sin ofte virtuelle form, og for mange er det f.eks. mere krænkende, at en person følger efter en på gaden end at vores e-post kommunikation bliver logget. Selvom digital teknologi væsentligt har øget overvågningen, herunder dens intensitet, og generelt skaber usikkerhed, er denne overvågning ofte ikke umiddelbart så nærværende som den ikke virtuelle overvågning, hvilket dog ikke er ensbetydende med, at den ikke overordnet virker mere intensivt end den synlige overvågning. Det er blot væsentligt at fremhæve, at overvågningen kan være tæt på den fysiske person, og dette eksemplificerer, at de anvendte midler kan vise hvor intensiv overvågningen er.

3.3 Åbent eller skjult

Et væsentligt moment er om overvågningen sker åbent eller hemmeligt. Det må tages i betragtning om den overvågede person ved eller har let ved at vide, at der sker overvågning eller om overvågningen sker skjult. Moderne teknologi giver gode muligheder for at foretage skjult overvågning. Selvom eksempelvis logningsordningen (i dansk ret, Bekendtgørelse

988/2006) har været meget omtalt og af mange er blevet fremhævet som privatlivskrænkende er den i realiteten skjult. Ordningen som den følger af direktiv 2006/24 er af EU Domstolen underkendt som uproportional[11], hvilket skyldes, at generel logning medfører registrering af oplysninger om de mange, der ikke har nogen kriminel intention, med henblik på at lokalisere oplysninger om de få personer, der kommunikerer med henblik på at udøve alvorlig kriminalitet; "nålen i høststakken". Overvågningen gennemføres skjult i den forstand, at man ikke kan se, at der logges, og det er de færreste, og det gælder også dem, som kender og er optaget af ordningen, der tænker på logning, når de eksempelvis sender en e-mail. Informationsteknologien er integreret i vores liv og det gælder også for dens skyggesider, selvom det jo ikke betyder, at disse uden videre skal accepteres.

3.4 Den overvågende

Det må endvidere tillægges betydning hvem der foretager overvågningen. Dette præger karakteren og ligeledes oplevelsen af den foretagne overvågning. Der kan groft skelnes mellem offentlige myndigheder og private virksomheder. For den enkelte person spiller det en rolle om der foreligger tillid til overvågeren eller det modsatte er tilfældet. I den konkrete situation kan det have betydning med hvilken samfundsmæssig legitimitet overvågningen foretages, herunder om den har et lovgrundlag eller andet retligt grundlag. Selv i et samfund som vores, hvor staten ikke ses som en fjende, er dette ikke ensbetydende med, at statslig overvågning umiddelbart er acceptabel for selv "en god stat" kan fejle eller intervenere for dybt i civilsamfundet.

3.4.1 Efterretningstjenester

I denne forbindelse er det nærliggende at fremhæve den overvågning, der foretages af efterretningstjenester. Der har som bekendt været stor opmærksomhed herom[12]. Overvågningen har i og for sig den samme karakter som når den udøves af andre instanser, men det kan alligevel bortlede et fokus på de grundlæggende problemstillinger at sætte et særligt stort søgelys på denne form for overvågning. Dette skyldes dels at temaet uvilkårligt tit bliver det betimelige i overhovedet at have efterretningstjenester dels at overvågningen er baseret på et særligt retligt grundlag. I dansk ret er der særskilt lovgivning om tjenesterne (PET/FE) med anvendelse af specielle tilsynsmyndigheder[13]. Persondataloven (§ 2, stk. 11) gælder ikke på dette område, idet dette er i overensstemmelse med EU databeskyttelsesdirektivet (45/96 artikel 3(2)) og i øvrigt ligeledes den kommende persondataforordning (artikel 2(2a)).

Værnet af national sikkerhed konstituerer en særlig verden, der altid har været præget af overvågning, og som "blot" har fået mere effektive midler til at foretage denne overvågning. Den er måske blevet mere nærværende for flere personer, men den har altid været til stede. Der er ikke nogen grund til at tro at denne verden vil forsvinde og selvom den bestemt ikke må negligeres bør denne overvågnings særlige og måske fascinerende baggrund ikke bortlede opmærksomheden fra den "ordinære" overvågning. Derfor holdes denne form for overvågning uden for i det følgende.

3.5 Stedet

Et yderligere moment af betydning for vurderingen af overvågning er hvor den finder sted. Det er nærliggende at foretage en opdeling mellem det offentlige og private rum, idet sidstnævnte retligt kan afgrænses til områder, der ikke er frit tilgængelige for enhver, jfr. herved straffelovens § 264a. Der kan yderligere være særlig grund til at udskille det internationale rum. Det er en følge af den moderne teknologi, at overvågningen i betydeligt mindre omfang end tidligere er nationalt forankret. Den kan komme alle steder fra. Det nationale rum er vel stadig dominerende, men med anvendelse af satellit overvågning og med internettets globale dimension er hele verden blevet åbent. Det er blevet lettere at se ind i og hente information ud af de enkelte nationale rum, hvis afsondrethed løbende bliver eroderet. Den meste overvågning er som nævnt fortsat national, men som udviklingstendens er den internationale dimension i kraftig vækst og væsentlig at være opmærksom på.

3.6 Den positive overvågning

Som fremhævet ovenfor er det endimensionalt at betragte al overvågning som et negativt fænomen, der må hindres og forebygges. Overvågning kan tjene gode formål ved at beskytte personen imod at blive udsat for et eller andet onde; f.eks. kriminalitet. Der kan være samfundsmæssigt fornuftige grunde til at gennemføre overvågning med den omkostning, at privatheden begrænses. I denne sammenhæng må betones, at privathed også i det offentlige rum er en værdi, der påkalder beskyttelse. Selvom man i dette

rum lettere kan ses og må acceptere dette betyder det ikke, at man altid skal kunne ses.

De følgende betragtninger er fokuseret på den overvågning, der negativt er orienteret imod det enkelte individ og som herudfra på en eller anden måde krænker det private. Det er denne form for overvågning, der aktualiserer spørgsmålet om der retligt eller faktisk kan gennemføres modforanstaltninger.

3.7 Overvågelighedsgrad
Det er ikke realistisk og lidt utopisk at forestille sig, at det er muligt at stoppe enhver overvågning, men der ikke tvivl om at den enkelte person kan gøre sig mere eller mindre overvågelig. Den enkeltes adfærd er stadig på mange måder betinget af egne indstillinger og viden, hvorfor det i en vis udstrækning er muligt at beskytte privatlivet. Dette kan ikke ske fuldstændigt og det er ikke realistisk for det normale menneske at hindre overvågningen ved et træde ud af samfundet. Dette vil kunne underminere demokratiet, der forudsætter deltagelse. Det er ikke et råd at begive sig ud på ødemarken eller at ophøre med at bruge teknologi. Sidstnævnte er kun et middel i ekstreme tilfælde således som det blev demonstreret ved de mange år, hvor den mest eftersøgte mand, Osama Bin Laden, forsvandt fra verden, fordi han ikke brugte nogen form informationsteknologi og derfor ikke gjorde sig sporbar.

4. Sikkerhed

Et nærliggende middel imod især den elektronisk betingede overvågning er anvendelse af former for sikkerhed, der opstiller barrierer omkring personrelateret information. Den moderne teknologi gør mennesket sårbart fordi den som udgangspunkt skaber åbenhed og uvilkårligt tilgængeliggør oplysninger for andre forudsat at disse råder over den nødvendige teknologiske ekspertise. Denne side af teknologien er velkendt, nærmest et nødvendigt onde, og midlet til at hindre eller i hvert fald begrænse åbenheden og til at understøtte værnet af det private område er den beskyttende teknologi. I megen teknologi er der indbygget en vis sikkerhed, men den er sjældent i sig selv tilstrækkelig til at forebygge persondatamisbrug. Det kan i denne forbindelse konstateres, at det er vanskeligt og i realiteten for de fleste umuligt at kontrollere sikkerheden. Dette er tilfældet, når den enkelte person selv behandler persondata, f.eks. i sociale netværk, men denne uigennemskuelighed er endnu mere påtrængende i den mere sædvanlige situation, hvor en eller anden instans behandler andres persondata.

I vidt omfang er den enkelte person ikke i stand til at beskytte sine egne data, selvom informationsteknologien stiller mange midler til rådighed og selvom gamle dyder som omhyggelighed, omtanke og påpasselighed stadig har betydning. Den digitale person kan udøve rettidig omhu, men dette forudsætter digital alfabetisme, som i realiteten kun et mindretal har[14], og det er meget let at komme i en udsat eller sårbar situation uden at ville det og endda uden at vide det. Det informationelle landskab er vidtstrakt og uigennemskueligt. Beskyttelsesopgaven må være placeret hos den instans, der har personoplysningerne i sin rådighed og som i persondataretten er kategoriseret som den dataansvarlige, jfr. yderligere hertil nedenfor. Som udgangspunkt skal datasikkerhed realisere et enkelt og overskueligt mål, der angiver, at kun autoriserede personer får adgang til de oplysninger de er autoriseret til og udelukkende anvender disse oplysninger til autoriserede formål. Den moderne teknologi har vanskeliggjort opfyldelsen af dette mål også selvom der udelukkende fokuseres på systemsikkerhed[15].

Der findes en mængde sikkerhedsteknologi, som den dataansvarlige kan vælge mellem og afpasse efter den databehandlingssituation, der skal beskyttes. Det er ofte vanskeligt at træffe dette valg, som er betinget af en række forskelligartede faktorer. Der er i det mindste to generelle problemer i denne forbindelse.

Det første vedrører omkostninger og er det mest ligetil af problemerne. Sikkerhed repræsenterer sædvanligvis en udgift for den dataansvarlige og spørgsmålet er hvor stor denne skal og bør være. Det renfærdige svar er at dette spørgsmål ikke er relevant fordi udgiften må være så stor, at der er etableret tilstrækkeligt effektivt virkende sikkerhed. Dette er i realiteten ikke et retningsgivende svar, idet det er en anerkendt almen interesse, at det må være muligt at anvende den moderne teknologi til persondatabehandling. Der må på denne baggrund i den praktiske verden foretages en konkret vurdering, som tilpasser udgiften til behandlingssituationen, herunder dennes formål og karakteren af de persondata, der behandles. Interessen i værnet af det private er således dif-

ferentieret og er tilpasset en formodning om graden af privathedsrisici. Sikkerhedsniveauet varierer og den dataansvarliges pris for at behandle andres data er forskellig. Under alle omstændigheder er der omkostninger og dette er i sig selv et problem for både offentlige og private dataansvarlige. Dette indebærer en fristelse, der fremmer en tilbøjelighed til i nogle tilfælde at vælge en billig og mindre sikker løsning.

Dette er baggrunden for at der i persondatalovens §§ 41-42 er fastsat en række regler om sikkerhed, idet de forpligtelser, som er fastlagt på lovniveau er forholdsvis overordnede og ikke indeholder konkrete anvisninger til den dataansvarlige. De fastsatte regler er for så vidt fleksible og tilpasselige til den teknologiske udvikling. På dette punkt er reguleringen i Danmark dog mere detaljeret end i mange andre EU lande eftersom vi i bekendtgørelse (528/2000) og vejledning (37/2000) har fastsat ganske detaljerede regler, som skal opfyldes af de dataansvarlige[16.] Disse regler begrænser til en vis udstrækning den dataansvarliges valgfrihed med hensyn til hvilke specifikke sikkerhedsforanstaltninger, som skal bringes i anvendelse med henblik på at opnå et forsvarligt sikkerhedsniveau. Et eksempel herpå er, at der ved behandling af følsomme persondata skal anvendes kryptering og foretages logning, idet et sådant almindeligt krav som nævnt ikke er fastsat i alle EU lande.

Nedenfor under 9 inddrages den forestående EU persondataforordning, der om nogle år vil udgøre det retlige grundlag frem for de i dag gældende danske regler[17]. Det kan overvejes om forordningen på dette punkt vil have positiv betydning, når det tages i betragtning, at den må formodes at ville medføre at sikkerhedsbekendtgørelsen vil blive ophævet. Forordningens sikkerhedsregler er overordnet udformet og der er dermed i en vis forstand tale om en begrænset harmonisering af sikkerhedsniveauet i medlemsstaterne. En egentlig harmonisering med et højt sikkerhedsniveau forudsætter, at EU Kommissionen i en såkaldt delegeret retsakt (forordning artikel 86) udformer detaljerede sikkerhedsbestemmelser således som vi kender dem i sikkerhedsbekendtgørelsen. Kun tiden vil vise om dette bliver tilfældet og under alle omstændighed vil der i en periode kunne opstå et vakuum. Når de nationale traditioner i medlemsstaterne tages i betragtning og når det kan lægges til grund, at detaljerede regler vil virke særdeles harmoniserende, kan en sådan regulering langt fra tages for givet. Udformningen af en retsakt med sikkerhedsregler vil i sig selv skabe en retspolitisk slagmark, hvor bl.a. de store amerikanske aktører (Facebook, Google, IBM, Microsoft, m.fl.) vil forsøge at påvirke reglernes indhold. Alt i alt foreligger der således en risiko for sikkerhedsreduktion.

Det andet problem forbundet med sikkerhed er, at den dataansvarlige ikke selv udformer de enkelte foranstaltninger. Den dataansvarlige kender oftest ikke teknologien og kan ikke forventes at have en sådan viden. Den enkelte sikkerhedsforanstaltning må derfor nødvendigvis i langt de fleste tilfælde købes udefra og den må ligeledes nødvendigvis installeres af særligt it kyndige personer. Det faktiske sikkerhedsniveau beror i betydelig udstrækning på tillid til disse aktører, og de fleste dataansvarlige er ikke i stand til at kontrollere, at alt er gjort på rette måde. Den dataansvarlige kan ikke vide om den indkøbte sikkerhed reelt er venlig eller fjendtlig over for persondatabehandlingen. NSA overvågningen har særligt tydeligt sat søgelyset på denne situation. Kryptering er eksempelvis en meget anvendt form for sikkerhed og i en del tilfælde, f.eks. ved transmission af følsomme persondata[18], er det som nævnt ovenfor i dansk ret en pligtig metode. Når der installeres kryptering kan leverandøren have placeret en bagdør, som medfører at oplysningerne, hvis tilgængelighed beror på kendskab til krypteringsnøglen, alligevel er blevet åbnet for andre, der således har mulighed for at foretage datamisbrug. Sådanne bagdøre kan endda være maskerede som programmeringsfejl og derfor se uskyldige ud såfremt den dataansvarlige alligevel skulle opdage dem.

Sikkerhed er et ideal og et mål, der da også i mange situationer bliver realiseret. Det er først og fremmest ved brug af sikkerhed, at persondataretten vender sig imod overvågning og dermed yder sit til at værne det private område. Sikkerhed er det primære middel imod at personoplysninger bliver anvendt til uønskelige former for overvågning. I mange situationer repræsenterer sikkerhed et brugbart værn imod overvågningen, men der er langt fra altid blevet skabt et uigennemtrængeligt skjold. Datasikkerheden bliver konstant udfordret og der er ingen grund til at nære illusioner om, at man på denne måde kan komme den negative overvågning til livs. Overvågeligheden er der og selv overholdelse af de bedste regler om sikkerhed kan ikke fjerne overvågningen fuldstændigt.

5. Persondataret

Retssystemets hovedmiddel imod overvågningen er persondataretten, idet der ikke findes en egentlig samlet overvågningsret[19]. Det er væsentligt fra starten at være opmærksom på, at persondataretten således som den manifisteres i persondataloven (429/2000) generelt vedrører betingelserne for lovlig behandling af personoplysninger og ikke i sin udformning er rettet specifikt imod overvågning. Denne aktivitet er blot en af et utal af måder, som personoplysninger kan behandles på. Persondatarettens formål er at fastlægge de betingelser og de vilkår, som den dataansvarlige skal opfylde for at få adgang til at behandle andre personers personoplysninger, jfr. også nedenfor. Det kan lægges til grund at disse krav skal være opfyldt for, at overvågning af persondata i digital form kan finde sted[20]. Det er således en central pointe i den gældende ordning, at enhver form for persondatabehandling forudsætter et retligt grundlag (hjemmel).

Persondataretten tilkendegiver, nutidigt i god tråd med menneskerettighedskonventionens artikel 8 om privatlivets fred, og EU charteret om grundlæggende rettigheder artikel 7 og 8[21] at personoplysninger er bærer af en menneskelig værdi. Persondata repræsenterer i vores tid det private, men persondatabeskyttelse er dog ikke fuldt ud det samme som privatlivsbeskyttelse. Databeskyttelse tager sigte på at hindre ikke proportional anvendelse af personoplysninger, men foretager ikke nogen egentlig markering af et privat område.

Persondataretten er i sin praktiske udformning baseret på en reguleringsmodel, der er orienteret imod den, som råder over personoplysninger ("den dataansvarlige"), og kun i mindre udstrækning imod den, som oplysningerne vedrører ("den registrerede")[22]. Det er den dataansvarlige som pligtsubjekt, der er reglernes adressat, og det er via den dataansvarliges lovlydige adfærd, at den registrerede som rettighedssubjekt opnår databeskyttelse. Brugen af denne model illustreres af den betydning, som samtykke tillægges[23]. Det følger af persondatalovens § 6, stk.1, § 7, stk.2, og § 8, at personoplysninger kan behandles på grundlag af et samtykke, der efter § 3 nr.8 skal være informeret, specifikt og frivilligt. Dette er dog kun en af flere muligheder, som den dataansvarlige kan vælge imellem, og samtykke er således ikke en nødvendighed eller en hovedregel, der først skal indrages af den dataansvarlige[24]. Som det ofte er konstateret indebærer persondataretten ikke nogen empowerment af den enkelte person, og det kan tilføjes, at en sådan anderledes reguleringsmodel end ikke har været overvejet i relation til forslaget til persondataforordning, der tematiseres nedenfor under 9.1.

På det konkrete niveau er spørgsmålet om persondataretten udgør et effektivt værn imod overvågningen. For en umiddelbar betragtning er dette ikke nogen selvfølge, men dette skyldes dog først og fremmest de svagheder, som generelt er knyttet til retlig regulering. Retten er ikke noget perfekt virkemiddel, som altid medfører en faktisk tilstand, som modsvarer den, der beskrives i reglerne, og dette gælder også for persondataretten. På papiret fremtræder persondataretten som en god form for regulering. Den er rettet imod og stiller krav til den dataansvarlige, som i denne sammenhæng er den, der foretager eller på hvis vegne overvågningen bliver foretaget.

6. Grundprincipper

Persondatabehandling kan kun iværksættes, såfremt en række grundlæggende principper, der er opregnet i persondatalovens § 5, bliver overholdt[25]. Denne bestemmelse kan karakteriseres som persondatarettens "grundlov" og er dermed centralt placeret i værnet af den informationelle privathed. Overvågning må være i overensstemmelse med god skik og selvom betydningen heraf kan være vanskelig at indkredse indebærer dette i det mindste, at den skal være fair og lovlig, dvs. ikke være i strid med andre retsgrundlag. Persondataretten spiller sammen med hele retssystemet. Datatilsynets vurdering af om en fremgangsmåde er i overensstemmelse med god skik kan indebære, at selv den i øvrigt lovlige behandling ikke kan finde sted. På denne måde virker bestemmelsen som en generalklausul.

Det er yderligere et krav, at persondatabehandlingen og dermed overvågningen skal være begrundet i et sagligt formål, og at de indsamlede oplysninger ikke senere må benyttes til et uvedkommende formål. Det er i sagens natur ikke uden videre klart hvad der er sagligt, men det er under alle omstændigheder forudsat, at der er en forbindelse mellem overvågningen og formålet med den type af aktivitet, som den overvågende instans udøver. Det kan diskuteres om dette indebærer nogen synderlig begrænsning i forhold til den overvågning, der foretages af professionelle

på grundlag af opdrag fra andre. Persondataretligt er dette dog alligevel tilfældet, idet overvågningsinstansen i så fald handler som databehandler[26] for opdragsgiver, og det er sidstnævntes formål, der udgør målestokken. Saglighedskravet kombineret med kravet om at al efterfølgende behandling skal være formålsbestemt har på samme måde som nogle af de principper, der omtales nedenfor, til formål at skabe transparens. Det skal være muligt for borgerne at forudse hvem der vil overvåge med henblik på hvilket formål. Dette er selvsagt et mål, der i praksis er svært at opfylde, men det er alligevel væsentligt, at aspirationen om transparens understøttes retligt.

Det er endvidere et krav, at der ikke sker overvågning af flere personoplysninger end det er nødvendigt for at opfylde overvågningens formål. Der må ikke indsamles såkaldt overskudsinformation, som måske vil kunne bruges på et senere tidspunkt ("just in case"). Det er ikke let i praksis at præcisere dette krav ud over de åbenlyse tilfælde. Grænserne mellem det umiddelbart anvendelige og det først senere relevante kan være særdeles flydende, hvortil kommer, at mange persondata formidler flere former for information. Princippet klargør på denne baggrund især hvor vigtigt det er, at overvågningens formål er klart og tydeligt formuleret. Dette er målestokken for om indsamlede oplysninger er relevante. På denne baggrund er det en af persondatarettens svagheder, at der ikke stilles klare og specifikke krav til formålsangivelsen. Den må ikke være helt udflydende, men den behøver heller ikke være særlig præcis. Viden om persondatabehandlingens formål er af denne grund ikke i dag tilstrækkeligt til at opstår den ønskelige transparens.

I almindelighed gælder der et krav om at der skal være proportionalitet mellem overvågningens formål og de indsamlede oplysninger. Dette krav vedrører ikke alene antallet af oplysninger eller deres relevans, men tager derimod først og fremmest sigte på de pågældende oplysningers egnethed til at realisere formålet. På et generelt plan skal den dataansvarlige således foretage en kvalitativ bedømmelse af oplysningerne. Proportionalitet er en norm, der gælder i EU retten generelt, men den er vanskelig at gøre helt præcis, selvom denne norm i konkrete tilfælde fungerer som en væsentlig rettesnor[27]. Proportionalitet er især væsentlig som følge af den moderne informationsteknologi, som tit medfører, at informationsindhentning kan sammenlignes med at skyde med spredehagl. Den moderne informationsteknologis force er dens evne til at håndtere store (nærmest uanede mængder) oplysningsmasser og at dybdesammenstille dem ("Big Data"), og dermed bliver den potentielle information, der kan udledes af oplysningerne, større end den kunne blive ved brug af manuel teknologi, især når hensynet til ressourceanvendelse tages i betragtning. Proportionalitet bliver dermed afgørende som en rettesnor med henblik på begrænsning af oplysningsanvendelsen. Dette har eksempelvis betydning i forhold til sekundær brug af persondata med henblik på markedsføringsformål. Der er løbende en risiko for, at der uden nogen særlig kritisk opmærksomhed indsamles oplysninger, som ikke er nødvendige for at realisere formålet. Det kan i denne forbindelse konstateres, at overvågning i de fleste tilfælde har masse karakter og således ikke i dens praktiske udførelse specifikt er orienteret imod en bestemt person. Det er i forhold til massen, at overvågningens proportionalitet skal vurderes.

I en parentes kan det i denne forbindelse fremhæves, at persondataretten beskytter privatlivet i forhold til enhver form for persondatabehandling og dermed også i relation til registrering. Den omstændighed, at nogle af overvågningens resultater ikke umiddelbart bliver benyttet, men blot bliver opbevaret, indebærer ikke, at proportionalitetskravet ikke skal opfyldes. Dette skyldes, at dataindsamling og registrering i sig selv skaber en risiko for at der på et senere tidspunkt kan ske persondatamisbrug. Der opstår en latent trussel om privatlivskrænkelser, som må søges forebygget. Sammenfattende er proportionalitet en generel forudsætning, der begrænser overvågningens omfang og karakter.

Blandt de almindelige principper finder vi også datakvalitet. Dette betyder, at de oplysninger, som overvågningen resulterer i, skal være korrekte og ligeledes ikke må være vildledende eller misvisende set i relation til formålet, der som nævnt ovenfor forudsættes at være sagligt. Når det tages i betragtning, at overvågning sædvanligvis er orienteret imod en flerhed af personer er dette et krav, som er særdeles vanskeligt at opfylde fuldt ud. Det kan dog have betydning i forskellige relationer. For det første må det tages i betragtning ved tilrettelæggelsen af udvælgelsesfasen. Der må dermed være en rimelig grad af sandsynlighed for, at de personer, som overvåges, vil levere oplysninger, som er relevante i forhold til overvågningens formål. Kvaliteten må således vurde-

res forudgående. For det andet indebærer kravet om datakvalitet, at den dataansvarlige må bedømme de konkret indsamlede oplysninger for at tage stilling til om de er korrekte. Når der er tale om masseoplysninger er dette ressourcekrævende og kvalitetskravet kan let forekomme urealistisk. I praksis er man opmærksom på dette og kravets styrke afhænger således af den konkrete situation, hvor der tages hensyn til oplysningernes følsomhedsgrad og hvor potentielt integritetskrænkende i forhold til de overvågede personer deres anvendelse kan være. Overvågningen må så at sige være farlig i forhold til det private for at der er grundlag for at stille et kvalificeret kvalitetskrav. Dette indebærer især i forhold til den kommercielt orienterede overvågning, at kvalitetskravet i realiteten i mange tilfælde i forhold til alle overvågede personer har forholdsvis begrænset betydning.

Endelig gælder der et tidsbegrænsningsprincip, som er relateret til den risiko, som registrering kan indebære. Det er fastsat, at oplysninger ikke må opbevares længere end de er brugbare i forhold til indsamlingsformålet. Der er ikke i persondataloven angivet bestemte frister, idet det som udgangspunkt er overladt til den dataansvarlige at skønne hvornår oplysninger skal slettes[28]. Princippet vedrører korrekte oplysninger og det bliver tit opfattet som ganske svagt, da dets overholdelse er vanskelig at efterprøve. Det tilføjes, at spørgsmålet om en ret til at blive glemt inddrages nedenfor under 9.

De almindelige principper er på mange måder persondatarettens væsentligste bidrag til reguleringen af adgangen til overvågning, men der er dog yderligere som nævnt ovenfor det fundamentale krav, at overvågning skal have hjemmel, som sædvanligvis må søges i persondatalovens §§ 6-8[29]. Når der elektronisk indsamles oplysninger må der således være et retligt grundlag. Den dataansvarlige skal sikre, at dette er tilfældet. Det er vigtigt at fremhæve, at der ikke er tale om et formaliseret krav i den forstand, at der skal ske underretning herom til tilsynsmyndigheden, Datatilsynet. Det kræver således ikke nogen tilladelse eller en anmeldelse at iværksætte overvågning af almindelige personoplysninger (§ 6), hvilket betyder, at Datatilsynet, ikke på denne måde har et overblik over den overvågning, der finder sted. Det er således lidt tilfældigt hvad der kommer frem til Datatilsynet. Dette skyldes ressourcemæssige hensyn og ønsket om at undgå et stort bureaukrati omkring anvendelsen af persondata. Det er dermed først i konkrete sager, at det bliver undersøgt om der foreligger den nødvendige hjemmel.

7. Oplysningspligt

Persondataloven forpligter den dataansvarliges til at opfylde de rettigheder, som loven giver borgerne[30]. Her kan der være grund til særligt at nævne oplysningspligten (§§ 28-29), der forpligter den dataansvarlige til at give information til hver enkelt person om formålet med dataindsamlingen samt sin egen identitet. Denne rettighed, som skaber det indledende grundlag for transparens, forudsætter ikke noget initiativ fra den enkelte person, der jo i mange tilfælde ikke ved, at der sker overvågning. Det forekommer ikke sandsynligt, at oplysningspligten bliver opfyldt i alle tilfælde og især ikke når der sker masseovervågning. Tværtimod sker dette nok forholdsvist sjældent.

Dette skyldes ikke nødvendigvis ond vilje, idet kendskabet til de persondataretlige regler gennemgående er forholdsvist lavt. Retsuvidenhed er i almindelighed en af den retlige regulerings svagheder så på dette punkt er persondataretten desværre ikke noget specielt. Overvågningen gennemføres ofte i det skjulte og det er derfor en væsentlig opgave at gøre oplysningspligten mere effektiv, jfr. også nedenfor om den kommende EU forordning.

8. Persondatarettens effektivitet

Det nu beskrevne er persondataretten som den er formelt, men som allerede antydet ovenfor er det et åbent spørgsmål om de forskellige regler også er en beskrivelse af situationen som den faktisk er. Spørgsmålet er om personoplysninger faktisk kun bliver anvendt således som det fremgår af reglerne. Det er en udbredt opfattelse, at de persondataretlige regler i praksis kun bliver overholdt i begrænset omfang[31] og i forhold til masse overvågning forekommer dette sandsynligt. Dette kan skyldes uvidenhed eller ond vilje og ligeledes at sanktionsniveauet i Danmark er lavt og lidet afskrækkende, men uanset baggrunden vil det på denne baggrund være forkert fuldt ud at sidestille persondatalovens regler med det virkelige liv[32].

Dansk ret gælder kun i Danmark og EU ret kun i EU, men internettet kender ingen grænser og overvågningen behøver ikke at være nationalt afgrænset. Det er

den i stadig mindre grad og kommer overvågningen udefra rammes den oftest ikke af de EU bestemte persondataretlige regler. Dette er eksempelvis tilfældet, når der indsamles oplysninger fra en hjemmeside, der ikke er etableret i et EU land. Der er situationer, hvor persondatalovens § 4[33] medfører, at dansk ret alligevel er anvendelig overfor en udenlandsk hjemmeside, men det er i praksis ganske sjældent. I realiteten er denne form for overvågning ikke sikkert begrænset retligt. Der er ikke nogen global eller international privathed. Selvom der findes mange, herunder internationalretlige[34], konstateringer af den betydning, som persondatabeskyttelse skal tillægges, er dette ikke ensbetydende med, at denne beskyttelse under det globale perspektiv i realiteten er anerkendt som en grundværdi, og de fleste af verdens lande har fortsat ikke en persondataretlig regulering, som blot tilnærmelsesvist nærmer sig niveauet i EU[35]. Det er nødvendigt med internationale aftaler, som ikke findes i dag. Nettets globale natur kan persondataretten ikke ændre på og dette må i en vis forstand tages til efterretning.

Den gældende persondataret kan ikke stoppe den krænkende overvågning, men i bedste fald begrænse og civilisere den. Det er væsentligt, at der ikke næres illusioner om hvad persondataretten kan opnå. Persondataretten fastlægger nogle retlige rammer, der kan føre til, at overvågningen trænger mindre ind i privatlivet, men disse rammer er hovedsageligt forholdsvist overordnede og forudsætter i betydelig udstrækning en positiv indstilling hos de overvågende myndigheder og virksomheder. Deres velvilje er i realiteten nødvendig for at loven kan have en positiv privatlivsbeskyttende virkning. Et blik ud i virkeligheden giver anledning til betydelig skepsis, eftersom overvågningen er stigende. Det er ikke sandsynligt, at den nutidige persondataretlige regulering tilstrækkeligt honorerer sin målsætning. På denne baggrund er der brug for en ny og mere præcis retlig regulering.

9. Forslaget til persondataforordning

Der er måske håb. Januar 2012 fremsatte EU Kommissionen et forslag til en persondataforordning[36], der erstatter databeskyttelsesdirektivet og de gældende love i medlemsstaterne. Direktivet er gennemført i 1995 lige før internettets folkelige gennembrud (World Wide Web) og i informationssamfundets tidsalder er dette nærmest forhistorie. Selvom forløbet, der er stærkt politiseret, er svært at forudsige er det for tiden sandsynligt, at forordningen i mere eller mindre ændret udgave bliver vedtaget i 2015 for herefter at træde i kraft 2017. Der bliver tale om lidt af en revolution inden for persondataretten selvom forordningen er en blanding af gamle og nye regler sammen med regler, der kodificerer den praksis, som er udviklet under direktivet. Langt fra alle i såvel den offentlige[37] som den private sektor ser frem til forordningen, men i mange kredse er der store forventninger til forordningen. Dette gælder ikke mindst i de kredse, der ønsker en så stærk beskyttelse af det private som nu engang muligt. Det er på ingen måde sikkert, at disse forventninger bliver indfriet og der venter givet privatlivsforkæmperne skuffelser fremover. Selvom der er et caveat er dog ingen tvivl om at forordningen vil være et nybrud i forhold til bl.a. muligheden for at forebygge overvågning og der er derfor god grund til at inddrage forordningsforslaget nærmere.

Selve det forhold, at der er tale om en forordning og ikke et direktiv vil utvivlsomt i sig selv have betydning. Persondataretten får en større tyngde og den får et stærkere apparat bag sig. Det samlede EU vejer tungere end de enkelte medlemsstater. Dette beror på de særtræk, der forbundet med en forordning, der er en del af det, som samlet betegnes supranational ret[38]. Den nationale ret erstattes af forordningen[39], som finder direkte anvendelse i de enkelte stater og som ikke må omformuleres til national ret. Dette er et statusløft, som demonstrerer at EU prioriterer persondatabeskyttelse, hvilket sender et væsentligt signal til den globale scene, der på denne måde søges påvirket. Borgernes værn imod datamisbrug bliver som udgangspunkt stærkere, når der reguleres ved en forordning.

Der kan anføres en række argumenter imod at anvende en forordning, idet det dels er tvivlsomt om alle dele af persondataretten grundet den udprægede brug af retlige standarder og sprogets flertydighed[40] kan harmoniseres tilnærmelsesmæssigt fuldt ud dels bør der tages hensyn til, at holdningen til persondatabehandling stadig i vidt omfang er knyttet til den nationale retskultur, som må tillægges væsentlig betydning. Den almindelige opfattelse af hvorledes staten og private virksomheder må anvende oplysninger om borgerne er forankret i politisk og retlig tradition, der ikke er den samme i alle medlemsstater. I forhold til disse momenter kan en forordning være forud for sin

tid og vise sig at være for ambitiøs, selvom det gældende direktiv har haft en vis udjævnende virkning. Der er tvivl og forbehold, men det er sandsynligt at slutresultatet alligevel bliver en forordning.

Det generelle spørgsmål er om forordningen vil blive en forbedring for borgernes databeskyttelse og styrke privatlivet overfor overvågningen eller om den i stedet skaber farlige illusioner herom. Dette er ikke et let spørgsmål at svare på i dag, hvor der i en vis forstand bliver tale om et kig i krystalkuglen. I almindelighed kan det konstateres, at der ikke i forordningen er medtaget regler, som specifikt er orienteret imod overvågning. Denne aktivitet er stadig "blot" en af mange former for persondatabehandling. Dette er i god overensstemmelse med persondataretlig tradition og er ikke nødvendigvis en mangel, men status quo på dette punkt er dog værd at bemærke.

9.1 Reguleringsmodel

Den grundlæggende reguleringsmodel er som nævnt ovenfor under 5 opretholdt, idet en ændring i denne henseende vist nok end ikke er blevet overvejet. Dette indebærer, at reguleringen fortsat er rettet til den dataansvarlige, der pålægges forpligtelser, som danner grundlaget for borgernes databeskyttelse. Den dataansvarlige er persondatarettens pligtsubjekt og er forordningens omdrejningspunkt således at alle dens fine regler er afhængige af om de dataansvarlige overholder dem i praksis. Den enkelte person er i realiteten ikke i stand til at kontrollere om dette er tilfældet og må basere sig på stærke datatilsyn. Den enkelte person er afhængig af den dataansvarlige, som ikke nødvendigvis er en ven, og personen er således, ofte til manges overraskelse, fortsat stillet indirekte i persondataretten. Forordningen medfører ingen egentlig empowerment af individet, selvom individet er rettighedssubjektet og selvom det private i betydeligt omfang er individuelt og personligt.

9.2 Rettigheder

Forordningen gentager i en lettere revideret form de rettigheder, der gælder i dag[41], og fastlægger herudover to nye rettigheder. Den ene er retten til portabilitet (artikel 18: ret til overdragelse fra informationssystem af tekst i bestemt struktureret form), der primært må karakteriseres som en forbrugerretlig rettighed og som er uden betydning i denne sammenhæng. Den anden er retten til at blive glemt (artikel 17(2-9))[42], som nu i et vist omfang er anerkendt af EU Domstolen i dommen vedrørende links i Google[43]. Selvom denne rettighed muligvis kan medføre en mindre begrænsning af overvågningens langsigtede virkninger medfører den i realiteten ikke den tryghed, som begejstringen i mange kredse for denne ret indicerer og som er en følge af, at retten til at blive glemt er blevet brugt som et af de bærende argumenter for at gennemføre forordningen. Den dataansvarlige er som i dag forpligtet til at slette korrekte oplysninger, der ikke længere er brugbare bedømt ud fra indsamlingsformålet (artikel 17(1)), idet det nye er retten til at få slettet links og retten til, at den dataansvarlige gør tredjeparter opmærksom på, at dette skal ske. Når der ikke er links er det besværligt at finde oplysningen, men den er stadig "out there", og er interessen stor nok kan den findes. Glemslen er ikke fuldstændig og det er fortsat således, at internettet hverken glemmer eller tilgiver. Retten til at blive glemt er i realiteten en ret til at blive husket med større besvær.

Bortset fra den dataansvarliges oplysningspligt forudsætter alle forordningens rettigheder, at borgeren tager et initiativ til at få dem aktiveret. Forudsætningen herfor er, at borgeren kender rettigheden og er stand til at handle. Denne forudsætning er i realiteten kun sjældent opfyldt. Dette forstærker indtrykket af, at forordningen ikke indebærer nogen empowerment af borgerne, der ikke er tildelt nye instrumenter, som de kan bruge med henblik på at sikre dem imod overvågningen.

Sådanne empowering instrumenter kunne være baseret på flere automatisk virkende rettigheder, der eksempelvis kan udformes som en præcisering af oplysningspligten således at overvågning, særligt i kontroløjemed, altid, eller kun undtaget på basis af specifikke betingelser, der må omfatte mere end den blotte lovhjemmel, skal gennemføres åbent og informeret. Manglende information bør ikke være årsagen til at overvågningen er skjult. En anden mulighed er automatisk indsigt inden for bestemte tidsintervaller. Sådanne ordninger er ressourcekrævende[44] og deres positive virkning må derfor i det mindste være sandsynlig, og her må det især overvejes om de kan medføre en form for informationsdød, hvor den enkelte person drukner i for megen information. Selvom der således er anden vej er det som tidligere fremhævet bemærkelsesværdigt, at sådanne former for empowerment ikke synes at have været taget i betragtning ved udformningen af forordningsforslaget.

9.3 Sikkerhed

Der er dog andre dele af forordningen, som kan have en gavnlig indvirkning på overvågningen. I denne forbindelse er der først og fremmest grund til at interessere sig for reglerne om datasikkerhed. God sikkerhed indebærer som fremhævet ovenfor et godt skjold imod overvågning og kan forordningen bidrage positivt hertil vil der være taget et væsentligt skridt i den rigtige retning. Samlet kan det i almindelighed konstateres, at der i forordningen sker en betydelig opprioritering af hensynet til sikkerhed, og det er påkrævet for den dataansvarlige at tildele dette hensyn stor vægt, bl.a. ved valget af den teknologi, der bruges til persondatabehandlingen. Dette fastslås på forskellige måder.

Overordnet er det i hvert fald symbolsk, at forordningen i artikel 22 betoner et princip om ansvarlighed ("accountability") således at den dataansvarliges opgave ikke blot består i at have god datasikkerhed, men også at demonstrere at dette rent faktisk er tilfældet. Det skal være tydeligt for omverdenen og den enkelte person, at oplysningerne befinder sig i en sikker havn. Der stilles på denne måde et større krav om en aktiv adfærd fra den dataansvarliges side end tilfældet er i gældende ret.

Dette eksemplificeres bl.a. af, at større private og alle offentlige dataansvarlige forpligtes til at have en lokal databehandlingsansvarlig, der i det daglige løbende bl.a. skal undersøge om sikkerheden er i orden og i modsat fald sørge for at dette bliver tilfældet (artikel 35-37). Denne ordning, der vist nok oprindeligt er udviklet i Tyskland, kan væsentligt bidrage til at databeskyttelsen er god de steder, hvor Datatilsynet ikke har øjne. Samtidig vil tilsynet få et netværk af kontaktled til de dataansvarlige.

Forordningens regler om den materielle sikkerhed byder også på nyt selvom en del af bestemmelserne er en form for kodificering af den praksis, der har udviklet sig under databeskyttelsesdirektivet samt det særlige e-persondata direktiv (2008/02 med ændringer). De egentlige sikkerhedskrav er ikke ændrede og på samme måde som i persondataloven beskrives disse kun på en generel måde. Forordningen øger den retlige styring af datasikkerheden, men er samtidig fleksibel og åben i relation til innovativ teknologi. Dette er nødvendigt fordi den teknologiske innovations tempo er sprint, medens lovgivningens er maraton.

Det er nyt, at den dataansvarlige forpligtes til ved persondatabehandlingens tilrettelæggelse at tænke fremtidsorienteret ved at opfylde principperne om privacy by design og privacy by default (artikel 23). Det har i mange år været en aspiration, at der på forhånd ved udformning af ny teknologi skal være taget højde for de privatlivskrænkelser, der vil kunne forekomme i forbindelse med brugen af personoplysninger. I forhold til den anvendte teknologi er det ønskeligt, at den er udformet på en privatlivsvenlig måde bl.a. ved anvendelse af "Privacy Enhancing Technologies". Dette hensyn skal som nævnt ideelt være indarbejdet i teknologien; "embedded privacy". Det fremtidsorientere hensyn har ligeledes betydning for indretningen af de organisatoriske og fysiske rammer omkring persondatabehandlingen[45]. Dette er ikke længere blot en aspiration, men bliver med forordningen en retlig forpligtelse. Det vil sikkert tage nogen tid inden disse principper slår igennem bredt, men understøttet af aktive datatilsyn vil dette kunne ske og medføre en forbedret sikkerhed. Dette er vel ikke ensbetydende med, at overvågning ikke kan og vil finde sted, men er denne form for sikkerhed på plads er det muligt, at overvågningen begrænses.

Ingen retlige regler bliver overholdt fuldt ud og de fastsatte regler er derfor ingen garanti imod at sikkerhedsbrud vil forekomme, idet dette også kan skyldes brugen af uforudsete privatlivsindtrængende teknologier (Privacy Invasive Technology). Forordningen (artikel 31-32) indfører derfor en stram procedure, der skal følges i sådanne situationer. Den dataansvarlige pålægges en meddelelsespligt når der sker sikkerhedsbrud, som kan medføre kompromittering af personoplysninger. Der skal gives meddelelse til Datatilsynet med oplysning om hvilke foranstaltninger, som er iværksat for at stoppe bruddet og udbedre de skader, der måtte være sket. Er der risiko for at der er sket væsentlige persondatakrænkelser, som kan have umiddelbare virkninger, skal også de pågældende berørte personer informeres direkte. Denne regulering tilstræber bl.a., at der skal være åbenhed omkring datasikkerheden og dermed skærper den også den dataansvarliges incitament til at have god sikkerhed. Det er således et velkendt fænomen, at mange dataansvarlige ikke ønsker, at det bliver kendt, at deres sikkerhed ikke i orden. Dette kan være skadeligt for virksomhedens eller myndighedens omdømme. Det er sandsynligt, at meddelelsespligten i sig selv vil styrke sikkerheden, idet den tilskynder den dataansvarlige til at undgå situationer, hvor denne forplig-

telse aktualiseres. For en god ordens skyld må det dog fremhæves, at det ikke er givet, at alle dataansvarlige vil overholde forpligtelsen, og at den selvsagt kun gælder for dataansvarlige, som er omfattet af forordningen. Hertil bør føjes, at virksomheder, der er omfattet af amerikansk ret i mange situationer vil være omfattet af en tilsvarende forpligtelse ("breach notification"), idet meddelelsen selvsagt her går til en amerikansk myndighed.

9.4 Sanktioner

Det gældende direktiv (artikel 24) pålægger medlemsstaterne at fastsætte sanktioner for overtrædelse af reglerne, men deres karakter og omfang fastlægger den enkelte medlemsstat selv. Dette har medført, at sanktionsniveauet er meget forskelligt i EU landene og Danmark ligger i den lave ende, idet der sjældent udmåles bøder, som overstiger 25.000.kr. Det kan ligeledes fremhæves, at persondatalovens § 70 giver hjemmel til at straffe private dataansvarlige og databehandlere for offentlige dataansvarlige, medens en offentlig myndighed kun kan straffes, såfremt den overtræder bestemte vilkår fastsat af Datatilsynet. I den offentlige sektor er sanktionsordningen baseret på, at en myndighed kan anvende disciplinære foranstaltninger over for de ansatte eller disse kan straffes for tjenesteforseelser i medfør af reglerne i straffelovens kapitel 16[46]. Den ikke samordnede sanktionsordning i medlemsstaterne kan medføre en uheldig form for forumshopping som følge af, at megen persondatabehandling ikke er stedbundet.

Forordningen indebærer et set med danske øjne væsentligt øget sanktionsniveau, der skal være harmoniseret. Straf kan benyttes (artikel 78), men det er først og fremmest ved anvendelse af administrative bøder (artikel 79), at dette mål søges opfyldt. Disse bøder kan anvendes også i den offentlige sektor og ud fra forordningsforslagets ordlyd vil der fremover være et egentligt persondataretligt myndighedsansvar. Blandt andet er overtrædelse af sikkerhedsreglerne omfattet og det kan blive særdeles dyrt for den dataansvarlige ikke at have sikkerheden i orden[47].

Det kan diskuteres hvor stor betydning dette vil få i praksis. Det kan konstateres, at brugen af sanktioner på en million eller mere euro i en række medlemsstater måske nok har virket afskrækkende, men det er alligevel tvivlsomt om de har medført en reduktion i antallet af datamisbrug[48]. Det er velkendt, at straf har en præventiv funktion, men det er ligeledes en almindelig erkendelse i strafferetten, at denne funktions virkning ikke bør overdrives. Risikoen for store bøder kan have betydning i forhold til persondatabehandling udført af mindre dataansvarlige, også selvom en del behandling udløses spontant, men i forhold til de større former for behandling, herunder den systematiske overvågning, forekommer dette mere tvivlsomt. I disse tilfælde bliver der snarere tale om en indkalkuleret risiko og omkostning. Selvom persondataretten nu skal tages mere alvorligt er dette ikke ensbetydende med at den bliver mere virksom. Det kan skabe en illusion om effektiv databeskyttelse at stole på, at de skærpede sanktioner vil disciplinere de dataansvarlige. Der er tale om et fremskridt, men man skal være varsom med at tro på dettes virkninger. Sanktionsordningen er på mange måder en ukendt faktor i den nye persondataret.

9.5 Sammenfatning

Sammenfattende er det på mange måder usikkert om persondataretsforordningen vil kunne begrænse overvågningen på nogen signifikant måde. Det er givet, at overvågningen ikke vil forsvinde, da dette ligger uden for rettens muligheder, men en begrænsning især som følge af de udvidede sikkerhedskrav vil naturligvis være en gevinst. Under alle omstændigheder skal man ikke tro, at den hellige grav er velforvaret og at forordningen vil ændre virkeligheden på en afgørende måde. Overvågningen vil fortsat kræve modkamp fra borgerne og meget hviler fortsat på aktive og forudseende datatilsyn. Dette gælder både for den overvågning, der har sin oprindelse i EU, og i særdeleshed for den, som udspringer internationalt.

10. Overvågning og privathed

Som nævnt tidligere er overvågning en samlet betegnelse for mange typer af aktiviteter, der for en dels vedkommende på varierende måde kan være indgribende overfor privatheden. Afhængig af dens karakter repræsenterer overvågning en trussel imod og et indgreb i privatheden. Graden af indtrængen i det private varierer og vurderingen af den enkelte overvågningsaktivitet er betinget af hensyn, der er orienteret imod individets interesse set i lyset af realiseringen af almene samfundsmæssige behov.

Bestemte former for overvågning kan være samfundsmæssig uønskelige, men dette er ikke altid tilfældet, jfr. nedenfor. I betydeligt omfang beror vurderingen af en overvågningsaktivitet af de græn-

ser omkring privatheden, som den enkelte person sætter. I disse tilfælde er rettens mission at give det enkelte menneske handlemuligheder. Det er ikke alle informationelle privatlivskrænkelser, som persondataloven eller andre dele af persondataretten kan gøre en indsats imod. Der er i det hele taget grund til at fremhæve, at denne indsats er generel og samfundsmæssigt betinget og dermed beror på en kollektiviseret opfattelse af det enkelte individs indstillinger. Persondataretten er i sidste instans en del af retssystemets almindelige understøttelse af demokratiet. Persondataretten anerkender, at det private har et personligt og individualistisk præg, men dens regler er desuagtet baseret på en generel opfattelse af grænsedragningen omkring privatheden.

Det har på denne baggrund betydning på hvilken måde den enkelte form for overvågning opfattes og opleves. Af betydning kan være om overvågningen virker indtrængende i det private. Det kan eksempelvis iagttages at tv-overvågning som udgangspunkt ikke begrænser den enkeltes i øvrigt lovlige aktivitetsmuligheder. Vi bevæger os i en vis forstand lige frit om vi er i kameraets øje eller dette ikke er tilfældet. Dette kan forklare den positive opbakning, som tv-overvågning nyder i dag. Den generelle logningsordning har været meget udskældt, men også den er et eksempel på overvågning, der ikke genererer og hvor det almindelige menneske ikke oplever sin privathed krænket. E-mailen sendes og modtages på samme måde uanset om den logges eller ej. På denne baggrund kan man udskille den form for overvågning, der ikke i almindelighed inddrager den overvågede person.

Den kommercielt orienterede overvågning har ligeledes undertiden denne karakter, men den kan også involvere personen via oplysninger, som personen selv tilvejebringer. Det har ligeledes væsentlig betydning, at sådanne former for overvågning via profilering og Big Data teknikker (datamining) resulterer i en umiddelbar indtrængen i form af direkte markedsføring og tilsvarende aktiviteter. Denne overvågning kan opleves som privatlivskrænkende, bl.a. fordi den er baseret på en personorienteret profilering. Den statsligt begrundede overvågning har i mange tilfælde en tilsvarende karakter, ikke mindst som følge af nutidig digitaliseret forvaltning, hvor den udbredte brug af samkøringer danner grundlaget for omfattende profiler over de enkelte borgere. Det er ikke alle borgere, der er bevidste herom, men kendes profileringen skaber den tit en oplevelse af utryghed og af at det private ikke er privat; Big Brother is watching you.

En særlig dimension tilføres af den internationalt orienterede overvågning, fordi denne i særlig grad forener fjernheden og nærheden. Der er stor afstand mellem overvågeren og den overvågede, og den tryghed det demokratisk styrede samfund tilvejebringer, er ikke altid til stede. Privatheden indplaceres i en fremmed og ukendt ramme, som er præget af en anderledes retskultur end den borgeren er fortrolig med. Den utryghed dette kan foranledige understøttes i vidt omfang af den teknologiske udvikling.

Disse forskellige former for overvågning søger persondataretten med større eller mindre held at civilisere i den forstand, at de indsamlede personoplysninger skal behandles med omsorg for det private. Selvom dette til en vis grad er en mission impossible er persondataretten desuagtet det bedste middel, som retssystemet kan stille til rådighed, og som fremhævet tidligere gør persondataretten privatlivet lidt bedre og det er derfor, at dens indretning og de ressourcer, der sættes bag den, er så væsentlig.

11. Persondatarettens betydning

Persondataretten yder sit til at civilisere brugen af personoplysninger, men den synes i en vis forstand at savne potens i forhold til den uønskelige overvågning. Så mørkt behøver billedet dog ikke at blive tegnet. Tænker man det scenario, at der ikke fandtes nogen persondataret, er det let at forestille sig, at overvågningen ville være langt mere omfattende end det er tilfældet i dag. Internettet er en fristende platform til udnyttelse af personoplysningers værdi og uden persondataretlig intervention ville nettet udvikle sig til at være det vilde vesten og borgerne ville ikke have et privat liv, hvor de kan være i fred. Et retligt ureguleret internet er et skræmmebillede. Persondataretten er et fint udviklet system og den har positive virkninger. Ikke mindst bidrager persondataretten til et fokus på overvågningens skyggesider og den fastholder det beskyttede privatliv som en væsentlig ledestjerne i informationssamfundet. På denne måde gør persondataretten nytte og derfor er det vigtigt, at den stærk.

Persondatarettens gode sider genspejler sig dog ikke fuldt ud i praksis og det er vigtigt ikke at nære illusioner herom eller at tro at persondataretten og

den tilknyttede primært strafferetlige beskyttelse af privatheden (straffelovens kapitel 27) kan gøre hele arbejdet alene. Der er alene tale om et bidrag til at begrænse overvågningen. Først og fremmest er det nødvendigt at persondataretten og informationsteknologien går hånd i hånd. Uden brug af privatlivsvenlig teknologi kan retten ikke nå eller nærme sig sit mål. The answer to technology is technology blev det sagt engang og selvom dette er lidt endimensionalt, da den privatlivsvenlige teknologi ikke kan stå alene, er det dækkende at svaret på overvågning ikke kun er retlig regulering. Det er på denne måde man bør forstå persondatarettens rolle i det overvågelige samfund.

12. Privathed i farezone

Uanset den beskyttelse, der følger af persondatarettens indsats, befinder privatheden i vores samfund sig i en farezone. Den angribes mange steder fra og den er udsat for mange risici. Der er klare konturer af et teknologisk præget Panoptikon, der fængsler privatheden og som potentielt kan aflive den. Advarselslamperne er tændte og politisk må udformningen af de kommende års persondataretlige regulering have høj prioritet.

Det er en kombination af retlig regulering, privatlivsvenlig teknologi, og højt menneskeligt opmærksomhedsniveau, som kan redde privatheden ud af den storm, som den befinder sig i. Denne indsats er nødvendig ikke blot nu, men primært i forhold til fremtiden, fordi det er en gammel erkendelse, at har man først tabt privathed kommer den kun meget sjældent tilbage. Privatheden bliver et kært minde, idet evigt ejes kun det tabte.

Vi må selv være os selv og værne om os selv som autonome personer med en privatsfære. Vi kan ikke blot iagttage og lade os betage af alt det vidunderlige, som informationsteknologien kan præstere. Vi må ikke lade os lulle ind i tilfreds passivitet for ellers ender vi der, hvor "no one dared disturb the sound of silence".

Noter

1. Paul Simon

2. Raymond Wacks: " The long search for a definition of "privacy" has produced a continuing debate that is often sterile and, ultimately, futile" (The Protection of Privacy, London 1980 p.10)

3. Formuleringen stammer oprindeligt fra erstatningsretten, men er kendt fra artiklen The Right to Privacy af Samuel Warren og Louis Brandeis i 4 Harvard Law Review (1890) p.193-220. Denne artikel er efter sigende den næstmest læste tidsskriftsartikel i USA.

4. Privacy and Freedom (New York 1967) p.31-39. - Denne bog har i øvrigt en fremtrædende placering i amerikansk litteratur om privatlivs- og databeskyttelse.

5. Karl Marx, Friedrich Engels: Det kommunistiske partis manifest: "I stedet for det gamle borgerlige samfund med dets klasser og klassemodsætninger får vi en sammenslutning, hvor hvert enkelts fri udveksling er betingelsen for alles fri udveksling" (citeret fra Marx/Engels: Udvalgte skrifter bind 1 (Forlaget Tiden, København 1973) p.47.

6. Susan Landau: Surveillance or Security (MIT Press, Massachusetts 2013) p.7: "We have become a mobile society, always on and always connected"

7. Disse medier karakteriseres af Andrew Keen: Digital Vertigo (New York 2012) p.2 som "that permanent self-exhibition zone of our digital age".

8. En forpligtelse for alle, som er fyldt 15 år, og som følger af lov 528/2012. Kun få, f.eks. de meget gamle, kan blive fritaget herfor.

9. I indeværende folketingssamling forventes et lovforslag, der vil give mulighed for på bestemte områder kun at sælge, såfremt der betales uden kontanter. Det såkaldte kontantløse samfund anes for alvor i horisonten, og forekomsten af forskellige former for virtuelle valutaer med bitcoins som det mest kendte eksempel illustrerer den styrke, der er forbundet med cyberspace.

10. Det følgende er til dels baseret på de momenter, der nævnes i Betænkning 1483/2006 om TV-overvågning p.114-15.

11. Se EU Domstolens afgørelse af 8.april 2014 (C-293/12 og C-594/12) - Dommens eneste konsekvens for dansk ret har hidtil alene været, at den såkaldte sessionslogning er blevet afskaffet.

12. NSA overvågningen, som bl.a. afdækket af Edward Snowden, er verdenskendt.

13. Se hertil Peter Blume: Rettens begrænsede muligheder i forhold til overvågning, Juristen 2013 p.251-54.

14. Tidsmæssigt befinder vi os i en art interregnum, hvor den yngre generation er digitale børn for hvem teknologien er selvfølgelig, og den ældre generation, opvokset i en anden verden, søger at lære teknologien.

15. Udover systemsikkerhed er fysisk sikkerhed og ikke mindst organisatorisk sikkerhed væsentlige momenter. Det er velkendt, at den menneskelige faktor i mange tilfælde er årsagen til mange af de sikkerhedsbrister, der forekommer. Disse to former for sikkerhed inddrages dog ikke nærmere her.

16. Formelt omfatter de nævnte retsforskrifter kun offentlige myndigheder, men i Datatilsynets praksis lægges til grund, at tilsvarende regler gælder for private virksomheder. Det falder uden for denne artikels rammer at vurdere om de fastsatte regler, der nu er gamle, er tilstrækkelige i betragtning af den teknologiske udvikling siden 2000, idet fokus her primært er på reguleringsformen.

17. Se hertil Peter Blume: Direktiv eller forordning i persondataretten, Juristen 2012 p.8-13.

18. I en parentes nævnes, at det er udpræget i den offentlige debat at anvende terminologien "personfølsomme data", men at dette ikke er en juridisk terminologi, og i øvrigt i mange tilfælde er medvirkende til at forvirre debatten, da udtrykket anvendes i flæng og tilsyneladende dækker alle former for personoplysninger.

19. De regler, der har betydning for om overvågning kan finde sted og i givet fald under hvilke betingelser er placeret i mange love, og der savnes for så vidt et samlet systematisk overblik over på hvilken måde denne problemstilling håndteres i dansk ret.

20. Ifølge persondatalovens § 1, stk.1 og 2, omfatter loven enhver form for elektronisk persondatabehandling samt behandling med henblik på manuelle registre, og i den private sektor tillige systematisk manuel behandling.

21. Artikel 8 er bemærkelsesværdig fordi den for første gang gør databeskyttelse til en selvstændig grundrettighed og ikke blot som traditionelt som en del af beskyttelsen af privatlivets fred.

22. I persondataretten tages ikke stilling til om nogen, f.eks. personen, ejer personoplysninger. Det er rådighedsretten, der er reglernes omdrejningspunkt.

23. I den specielle persondataret som den udfoldes i sektorlovgivning, f.eks. sundhedsloven, kan (informeret) samtykke være tillagt særlig betydning, men der kan iagttages en tendens til, at samtykke som en hovedregel i stigende omfang ledsages af undtagelser.

24. Der kan dog være tilfælde, hvor det følger af god skik, jfr. § 5, stk.1, at der bør indhentes et samtykke.

25. Se nærmere hertil Peter Blume: Databeskyttelsesret (4.udgave København 2013) p.138-154.

26. I persondataloven er det anerkendt, at den dataansvarlige kan have brug for bistand og den, som på den ansvarliges vegne udfører behandlingen betegnes en databehandler, jfr. § 3 nr.5.

27. Et eksempel er EU Domstolens dom vedrørende logningsdirektivet, der på grundlag af en proportionalitetsbetragtning blev erklæret ugyldigt, jfr. note 9 ovenfor.

28. I forhold til tv-overvågning er der dog i § 29a, stk.2 fastsat en slettefrist på 30 dage, jfr. nærmere om denne regel og undtagelsen i stk.3 Peter Blume: TV-overvågning (København 2008) p.109-16.

29. Persondataloven er en lov på samme niveau som andre love, hvilket betyder, at hjemlen også kan

fremgå af andre love som eksempelvis sundhedsloven forudsat at databeskyttelsesdirektivet er overholdt.

30. Udover den i teksten nævnte oplysningspligt har borgerne ret til indsigt, ret til at få korrigeret ukorrekte oplysninger, indsigelsesret i forhold til specifikke individuelle situationer, samt en særlig indsigts- og indsigelsesret i forhold til fuldt automatiserede afgørelser baseret på persondata. Se i det hele persondatalovens §§ 30-40.

31. Dette dokumenteres af utallige EU undersøgelser herom.

32. Dette er en gammel erkendelse i retsvidenskaben, jfr. herved Alf Ross: Om ret og retfærdighed (København 1953) p.30, hvorefter "den, der kun kender normerne ved ikke meget om den korresponderende sociale realitet".

33. Ifølge stk.3 vil indsamling af oplysninger fra Danmark fra en udenlandsk hjemmeside være omfattet af loven, såfremt indsamlingen er rettet imod danske oplysninger, f.eks. fordi hjemmesiden er på dansk. - I almindelighed gælder loven ikke i de tilfælde, hvor der fra Danmark mere tilfældigt afgives oplysninger til udenlandske hjemmesider.

34. Ofte er internationale dokumenter udformet meget overordnet og i realiteten lidet dirigerende. Et eksempel er resolution om The right to privacy in the digital age udstedt af tredje komite under 68 FN generalforsamling (november 2013), hvor det smukt som henstilling til staterne i punkt 4.1. anføres, at disse opfordres "to respect and protect the right to privacy, including in the context of digital communication". Det forekommer svært ikke at skrive under på dette.

35. Dette forhold er baggrunden for de særlige regler om internationale dataoverførsler, jfr. persondatalovens § 27.

36. KOM 2012 (11) af 25.1.2012.

37. En del medlemsstater, herunder i hvert fald oprindeligt Tyskland, vil foretrække, at den offentlige sektor reguleres ved et direktiv, som i mindre omfang end en forordning intervenerer i statens aktiviteter, der opfattes som tæt forbundet til den enkelte medlemsstats suverænitet.

38. En retlig regulering, der adskiller sig fra national ret og folkeret via den suverænitet, som medlemsstaterne har afgivet til EU. Hos os inden for rammerne af grundlovens § 20.

39. Dette gælder principielt for alle persondataretlige regler, men det er muligt, at der i den endelige forordning vil blive åbnet for undtagelser i forhold til visse særlove, selvom dette vil svække den tilstræbte harmonisering.

40. De 24 officielle sprog er politisk nødvendige, men kan være retligt problematiske.

41. Ret til information, ret til indsigt, ret til korrektion af forkerte data, ret til indsigelse, og ret til indsigt/indsigelse i forhold til fuldt automatiserede afgørelser.

42. For en nærmere analyse af denne kontroversielle rettighed se Peter Blume: Retten til at blive glemt, Juristen 2013 p.117-23.

43. C 131/12 af 13.maj 2014. Ifølge dommen kan en person henvende sig til udbyderen af en søgemaskine og under bestemte omstændigheder have ret til at få et link, men altså ikke oplysningen, fjernet og dermed gjort oplysningen mindre sporbar. I dommens præmis 100(3) fastslås således pligten til "at fjerne link til websider, som er offentliggjort af tredjemand og indeholder oplysninger vedrørende denne person, også i tilfælde, hvor dette navn eller disse oplysninger ikke forudgående eller samtidig slettes fra disse websider, og i givet fald selv når offentliggørelsen på disse sider i sig selv er lovlig."

44. I persondataretten må der generelt tages stilling til hvor høj en pris den dataansvarlige skal betale for at behandle personoplysninger.

45. Se om hvorledes særligt hensynet til privacy by design kan have betydning i den fysiske verden Peter Blume, Janne Rothmar Herrmann: Retlig regulering af privatlivsbeskyttelsens infrastruktur, Ugeskrift for Retsvæsen 2010 p.298-302. Et eksempel er enestue overfor flersengsstuer på hospitaler.

46. Se nærmere om denne problemstilling, Peter Blume: Offentlige myndigheders persondataansvar, Ugeskrift for Retsvæsen 2014 p.337-341.

47. Det kan anmærkes, at Europa Parlamentet ikke blot støtter denne linje, men ønsker den væsentligt skærpet således at den maksimale bøde hæves fra en til to millioner euro. Det er dog tvivlsomt om dette bliver slutresultatet.

48. Der findes vist nok ikke nogen dybtgående undersøgelse heraf om end det er indtrykket i England, at der en præventiv virkning. I en vis forstand fægter denne del af forordningen i blinde.