I en højere sags tjeneste

Afvejningen mellem overvågning og privatliv i en retlig kontekst

Af Lars Bo Langsted & Søren Sandfeld Jakobsen

Abstract

Artiklen behandler ud fra en retsdogmatisk metode nogle af de grundlæggende problemstillinger, regler, principper og hensynsafvejninger, der gælder, når staten eller private virksomheder vil gennemføre overvågning af borgerne og dermed gøre indgreb i retten til privatlivets fred. Særlig fokus er på den digitale overvågning. Det konkluderes bl.a., at de gældende regler og retspraksis anerkender, at der konkret kan være andre interesser, det er vigtigere at varetage end retten til at kommunikere uden overvågning. For at disse legitime undtagelser ikke skal kunne udnyttes til en intetsigende og reelt altomfattende carte blanche til myndighederne, har domstolene dog også opstillet en række krav, dels til udformningen af regler, der giver hjemmel til overvågning, dels til den måde, disse regler administreres på af de relevante myndigheder. Retsstillingen er dog langt fra klar, og der er følgelig behov for yderligere forskning på området.

Lars Bo Langsted, Professor,
International Economic Crime and Cybercrime Research Centre, Juridisk Institut, Aalborg Universitet (lbl@law.aau.dk)
Søren Sandfeld Jakobsen, Professor,
International Economic Crime and Cybercrime Research Centre, Juridisk Institut, Aalborg Universitet (ssj@law.aau.dk)

1. Indledning

Borgernes ret til privatliv (herunder kommunikationshemmelighed og persondatabeskyttelse) er et grundlæggende retsprincip, der er beskyttet i både grundloven, Menneskerettighedskonventionen og EU-retten.[1] I ingen af disse 3 retssystemer er retten til privatliv dog ubegrænset. Retten kan således under visse omstændigheder vige til fordel for samfundsmæssige hensyn, der af lovgiver anses for mere væsentlige, fx hensynet til kriminalitetsbekæmpelse og statens og borgernes sikkerhed. Som følge heraf er der i Danmark en række love på forskellige samfundsområder, der hjemler adgang for myndighederne, fx politiet og efterretningstjenesterne, til at gennemføre forskellige former for overvågning af borgerne.

Med udviklingen inden for telekommunikation, digital teknologi og internettet er de tekniske muligheder for at overvåge borgerne, fx ved adgang til e-mails eller registrering og overvågning af tele- og internetkommunikation, blevet væsentligt forøget. Det har afstedkommet vedtagelse af flere lovregler, der inden for forskellige samfundsområder hjemler overvågning, eller har betydet, at eksisterende regler, der hjemler fysisk overvågning af den ene eller anden karakter, ved fortolkning af de relevante myndigheder udvides til også at omfatte digital overvågning.

Det er dog langt fra altid klart, om de forskellige regler, der giver adgang til overvågning, opfylder de betingelser for at gøre undtagelse fra det grund-

læggende forbud mod privatlivskrænkelse, der kan udledes af de grundlæggende regler og relevant domstolspraksis. Det skyldes igen, at det på grund af undtagelsernes brede og vage karakter ikke er klart, præcist hvad disse betingelser er og hvordan de skal anvendes i lyset af den digitale udvikling og internettets fremkomst. Disse spørgsmål er heller ikke, eller kun meget sparsomt, behandlet i den juridiske teori. Ligeledes er det langt fra klart, om - og i givet fald i hvilken udstrækning - private (fx udbydere af sociale medier på internettet) kan gennemføre overvågning via internettet eller andre telekommunikationsnetværk, fx for at undgå, at deres tjenester anvendes til ulovlige formål.

Forholdet mellem retten til privatlivsfred på den ene side, og adgangen til at gennemføre overvågning på den anden side, er således i juridisk henseende komplekst og præget af betydelig retsusikkerhed - og kalder derfor på mere systematisk forskning.[2] Henset til nærværende tidsskrifts tværfaglige karakter er formålet med artiklen dog alene på et mere overordnet plan at belyse nogle af de grundlæggende problemstillinger, regler, principper og - ikke mindst - hensynsafvejninger, der præger dette nye og vanskelige retsområde.

Indledningsvist diskuteres begrebet overvågning i juridisk henseende. Herefter præsenteres de væsentligste retsregler om overvågning tillige med de undtagelser, der gælder til disse regler, bl.a. for herigennem og ved inddragelse af retspraksis at undersøge, om der - på tværs af de forskellige og meget spredte regelsæt - kan udledes nogle generelle principper for, hvilke betingelser der skal være opfyldt, for at en given regel, der på et konkret samfundsområde hjemler adgang til overvågning, er i overensstemmelse med den grundlæggende ret til privatlivsfred, kommunikationshemmelighed og persondatabeskyttelse. I den forbindelse vil reglerne vedrørende politiets og efterretningstjenesternes overvågning blive særligt behandlet, herunder det under Forsvarets Efterretningstjeneste etablerede Center for Cybersikkerhed. Herefter undersøges spørgsmålet om privates adgang til at foretage overvågning. I den afsluttende konklusion og perspektivering vil der blive fremdraget en række konkrete problemfelter, der lægger op til mere detaljeret juridisk forskning på området.

2. Begrebet overvågning i juridisk betydning

Begrebet "overvågning" er ikke defineret i lovgivningen og har således ikke noget fast, entydigt juridisk indhold. I tv-overvågningsloven,[3] som er den eneste speciallov om overvågning, er tv-overvågning defineret som "*vedvarende eller regelmæssigt gentagen personovervågning ved hjælp af fjernbetjent eller automatisk virkende tv-kamera, fotografiapparat eller lignende apparat*", jf. § 1, stk. 2. Overvågning vedrører således det fænomen, at andre systematisk - dvs. på en forud fastlagt måde (fx via tv-apparatur, logning af teledata, software, webtjenester osv.) og med en vis tidsmæssig kontinuitet eller regelmæssighed - følger med i vores gøren og laden, herunder kommunikation, og på den måde udøver en form for kontrol med os, der indskrænker vores privatliv.[4]

Et andet karakteristikum er, at der ofte er tale om "masseovervågning", der ikke er rettet mod en specifik person (og som sådan kunne være i strid med dennes rettigheder), men er rettet mod samtlige personer, der fx passerer et givet sted eller foretager den samme handling, fx foretager et mobilopkald. I så fald vil det ikke (i første omgang) være den enkeltes fred, der krænkes, men alle borgeres kollektive fred, fordi det er denne, der på denne måde krænkes.[5]

Udtrykt retligt kan man på den baggrund måske sige, at overvågning omfatter alle handlinger, der går ud på systematisk at indsamle oplysninger om en eller flere personer på en måde, som - hvis det ikke har et særligt hjemmelsgrundlag - ville udgøre en krænkelse af retten til privatlivets fred, således som denne ret er beskyttet efter lovgivningen, herunder EMRK art. 8, straffeloven og persondataloven (jf. om disse regler nærmere nedenfor).[6]

Problemet med en sådan definition er, som uddybet nedenfor, at begrebet privatliv efter de nævnte regler er meget bredt og ikke har noget bestemt, afgrænset indhold.[7] Ved således at definere et uklart og vagt begreb ud fra et andet vagt begreb bliver definitionen selvsagt vanskelig at operere med i praksis. Hertil kommer, at vurderingen af, om en given handling udgør en ulovlig overtrædelse af de relevante regler, i sig selv er uhyre vanskelig, idet reglerne, som det vil fremgå nedenfor, er præget af undtagelser og skønsmæssige afvejninger, der gør retsstillingen svært gennemskuelig. Definitionen kommer herved til at hvile på en retlig kvalificering, som ikke blot er

vanskelig, men som også er konkret og til syvende og sidst op til domstolene, herunder Menneskerettighedsdomstolen, at foretage. Dette gør definitionen endnu mere problematisk.

Vælger man med disse betænkeligheder in mente alligevel at lade det grundlæggende menneskeretlige princip om retten til privatlivsfred være i det mindste et udgangspunkt for fastlæggelsen af overvågningsbegrebet i retlig henseende, jf. definitionen oven for, har det den metodiske fordel, at man derved yderligere - i hvert fald på et overordnet plan - kan indkredse begrebet ud fra de efterhånden mange bestemmelser rundt omkring i lovgivningen, der - om end ordet overvågning som regel ikke anvendes - på den ene eller anden måde udgør undtagelser til retten til privatlivets fred (herunder retten til persondatabeskyttelse) ved at give hjemmel til systematisk indsamling og registrering, af oplysninger - historiske eller aktuelle - om personers gøren og laden. Ved "systematisk" forstås som nævnt, at overvågningen sker vedvarende eller regelmæssigt ud fra et på forhånd fastlagt mål og nogle på forhånd fastlagte kriterier - i modsætning til en enkeltstående eller tilfældig indsamling af oplysninger.

Som eksempel på lovregler, der giver hjemmel til overvågning og derved indskrænker privatlivets fred, kan nævnes reglerne i retsplejelovens kap. 71, der netop bærer overskriften "indgreb i meddelelseshemmeligheden". Disse regler giver politiet hjemmel til at udøve forskellige former for overvågning af folks kommunikation med hinanden, herunder ved telefonaflytning og e-mail- og internetovervågning. For at værne retssikkerheden og sikre, at bestemmelsen ikke misbruges, er der dog en række betingelser, der skal være opfyldt. Reglerne omtales nærmere nedenfor sammen med den såkaldte logningsbekendtgørelse og reglerne om Center for Cybersikkerhed, der begge - i lighed med retsplejelovens kap. 71 - giver hjemmel til, at staten kan gøre indgreb i kommunikationshemmeligheden og persondatabeskyttelsen for at værne om et højere gode, nemlig efterforskning og opklaring af kriminalitet og beskyttelsen af rigets sikkerhed.

I de nævnte eksempler er det som sagt staten, der - evt. via private (fx teleselskaber) - gennemfører overvågning. Overvågning som defineret her - og i almindelighed - er imidlertid ikke begrænset til at være noget, som kun offentlige myndigheder gør brug af. Det er dog formentlig primært statens overvågning af borgerne, som mange forbinder med begrebet overvågning, og det er da også denne relation, der mest fokuseres på i nærværende sammenhæng. Internettet og den digitale teknologi har imidlertid gjort det muligt også for private at udøve overvågning, og dette sker i stigende grad, fx i form af webtjenester, der overvåger deres brugeres adfærd, eller arbejdsgivere, der overvåger deres ansattes e-mail- og internetkommunikation. Privates overvågning af hinanden sker også i stigende grad ved opsætning af tv-overvågningskameraer, jf. den oven for nævnte tv-overvågningslov[8]. Fokus i denne artikel er dog på overvågning via internettet og andre elektroniske kommunikationsmidler. Det skal tilføjes, at overvågning - og det dertil hørende indgreb i privatlivets fred - kan ske på mange andre måder end ved brud på kommunikationshemmeligheden, fx ved overvågning af brug af kreditkort, jf. den nok så omtalte Se og Hør-sag, eller ved adgang til offentlige registre med følsomme data vedrørende eksempelvis sundhedsoplysninger, straffeoplysninger, NemID-konti osv.

Ud over at antage mange forskellige former kan overvågning således også udøves af både offentlige og private virksomheder. Dette rejser en række retlige og retspolitiske spørgsmål, herunder først og fremmest om der er grundlag for og hjemmel til det pågældende indgreb, altså om en given overvågning overhovedet er lovlig, og i bekræftende fald hvor langt hjemlen rækker - og bør række i et retssamfund.

3. Beskyttelse af retten til privatlivets fred

3.1 EMRK art. 8

Det er den grundlæggende ret til privatlivets fred, herunder beskyttelse af persondata (der anses at udgøre en del af en persons privatliv), der udgør det retlige bolværk mod overvågning. Denne grundret er cementeret i både national ret, folkeretten og EU-retten, og fremgår således forskellige steder i lovgivningen. På folkeretligt plan er det Den Europæiske Menneskerettighedskonvention, EMRK, der i artikel 8 fastslår, at enhver har ret til respekt for sit privatliv og familieliv, sit hjem og sin korrespondance (herunder kommunikation, fx via telefon og internet). Som allerede nævnt er selve begrebet "privatliv" ikke nøje afgrænset efter art. 8. Menneskerettighedsdomstolen har udtrykkeligt bemærket, at privatliv er et bredt begreb, som det hverken er muligt eller nødvendigt

at definere udtømmende,[9] og at begrebet efter en konkret vurdering kan omfatte såvel en persons fysiske og psykiske integritet som en persons fysiske og sociale identitet.[10]

3.2 EU-retten
I EU-retten fremgår det af EU's charter om grundlæggende rettigheder[11] art. 7, at enhver har ret til respekt for sit privatliv og familieliv, sit hjem og sin kommunikation, og art. 8 supplerer ved at fastslå, at enhver har ret til beskyttelse af personoplysninger, der vedrører den pågældende. I modsætning til EMRK art. 8, der også omfatter persondatabeskyttelsen, er denne i EU-charteret således frigjort fra retten til privatlivets fred og udskilt i en særlig bestemmelse. Bortset herfra er betydningen og rækkevidden af EU-charterets rettigheder den samme som efter EMRK, jf. EU-charterets art. 52, stk. 3.

Det bemærkes i den forbindelse, at charteret kun er anvendeligt inden for de områder, hvor EU i forvejen har reguleret,[12] men da overvågning som regel indebærer behandling af persondata, som er forholdsvis tæt reguleret i EU-retten via to persondatadirektiver (det generelle persondatadirektiv henholdsvis e-datadirektivet, der særligt vedrører behandling af persondata i telesektoren),[13] vil charteret formodningsvis have betydning som retskilde i forhold til vurderingen af en given overvågningsaktivitet, jf. også nedenfor om EU-Domstolens tilsidesættelse af det såkaldte logningsdirektiv. Omvendt falder fx efterretningstjenesterne helt uden for EU's kompetenceområde, hvorfor EU-charteret ikke er anvendeligt på den overvågning, der finder sted i regi heraf. Denne begrænsning gælder ikke for Menneskerettighedskonventionen.

Som nævnt omfatter den EU-retlige regulering også de to førnævnte persondatadirektiver, der til sammen udgør en forholdsvis tæt regulering af adgangen til at behandle persondata, og som netop har til formål at beskytte den del af området for privatlivets fred, der vedrører behandling af persondata, herunder når denne behandling sker ved brug af elektroniske kommunikationsmidler, fx mobiltelefon, internet mv. Forebyggelse af overvågning gennem en stærk persondatabeskyttelse er også indarbejdet i andre EU-direktiver, fx betalingstjenestedirektivet,[14] der således supplerer det generelle persondatadirektiv.

3.3 Dansk ret
I national dansk ret er retten til privatlivets fred - og dermed værnet mod overvågning - for det første beskyttet i grundlovens § 72. Beskyttelsen omfatter dog kun tre typer af indgreb, nemlig husundersøgelse, beslaglæggelse og undersøgelse af breve og andre papirer samt post- og kommunikationshemmeligheden. Hertil kommer, at beskyttelsen efter § 72 ikke er særlig stærk, idet bestemmelsen - udover at forudsætte, at indgrebet har hjemmel - alene indeholder et krav om, at et indgreb kræver retskendelse, og det endda kun, hvis dette ikke ved lov er fraveget. En sådan fravigelse kan ifølge § 72 kun ske i "særegne tilfælde", men der er talrige eksempler rundt omkring i lovgivningen på, at kravet om kendelse konkret er fraveget.[15] I forhold til påberåbelse af retten til privatlivsfred som grundrettighed er det som følge heraf som oftest ikke grundlovens § 72, men EMRK (og eventuelt EU-charteret), der gøres gældende. Af samme årsag vil grundlovens § 72 ikke blive behandlet mere indgående i nærværende sammenhæng.

På almindeligt lovsniveau beskytter straffeloven mod forskellige former for privatlivskrænkelser, jf. straffelovens §§ 263-264 d, der bl.a. omfatter brud på brev- og kommunikationshemmeligheden, hacking, aflytning, at skaffe sig adgang til et ikke frit tilgængeligt sted (herunder efter omstændighederne virtuelle rum på internettet, fx lukkede profiler på sociale medier og tjenester) eller fotografere personer på et ikke frit tilgængeligt sted. Også den handling, der består i at videreudnytte oplysninger, der er skaffet ved en privatlivskrænkelse, er strafbar, ligesom det er strafbart uberettiget at videregive oplysninger (også selv om disse måtte være lovligt fremskaffet) om en andens private forhold "under omstændigheder, der åbenbart kan forlanges unddraget offentligheden".[16] Overtrædelse af reglerne straffes med bøde eller fængsel, der i grove tilfælde kan give helt op til 6 år. Civilretligt kan en overtrædelse også udløse en tortgodtgørelse efter erstatningsansvarslovens § 26. Der er dog i dansk retspraksis ikke tradition for særlig store tortgodtgørelser for fredskrænkelser.

Som nævnt omfatter straffelovens regler om privatlivets fred kun visse, bestemte fredskrænkelser. Det er fx kun ulovligt efter straffeloven, hvis man bruger et apparat til at aflytte personer, der befinder sig på en offentlig gade[17], men ikke hvis man ligger i skjul og tager billeder af deres ophold samme sted.[18] Desuden kræver overtrædelse af straffelovens regler generelt,

at der er handlet forsætligt, hvilket kan være svært at bevise. I praksis er det derfor langt fra altid, at straffelovens regler om fredskrænkelser kan anvendes på en given overvågningsaktivitet. Dette medfører, at lovligheden heraf ofte alene omfattes af persondataloven,[19] der derfor er en uhyre central lov i forhold til overvågning og privatliv.

Persondataloven implementerer det generelle persondatadirektiv, mens det særlige direktiv om behandling af personoplysninger og beskyttelse af privatlivets fred i den elektroniske kommunikationssektor (e-datadirektivet) er implementeret i telelovgivningen.[20] Persondataloven gælder for al behandling af personoplysninger, hvad enten der er tale om følsomme oplysninger eller ej. Herved har loven et lidt bredere anvendelsesområde end EMRK art. 8, der formentlig kun gælder for personoplysninger, som er følsomme eller dog har en tæt tilknytning til det private liv eller rum.[21] I modsætning til straffelovens regler om fredskrænkelser, der kan fraviges ved anden lov, kan persondataloven som udgangspunkt kun fraviges ved anden lov, hvis denne anden lov giver den registrerede en *bedre* retsstilling end persondataloven, jf. § 1, stk. 2. Det gælder dog ifølge lovforarbejderne ikke, hvis den dårligere retsstilling har været tilsigtet og i øvrigt ikke strider mod det bagvedliggende persondatadirektiv.[22] Realiteten er derfor, at dansk lovgivning godt kan indskrænke de rettigheder, der følger af persondataloven, medmindre dette vil være i strid med persondatadirektivet.

Persondataloven omfatter altså "behandling" af oplysninger, hvilket ikke blot er den bearbejdning, der sker af allerede eksisterende data, men også indsamlingen af disse data.[23] Hermed er persondataloven, som nævnt, helt central, også når spørgsmålet er at påse, om en given overvågning, der jo har til formål at indsamle data om personer, jf. ovenfor, har fornøden hjemmel og/eller kræver en særlig tilladelse.

Persondatareguleringen udgør et værn mod vilkårlig overvågning, idet den opstiller et krav om, at der skal være hjemmel i reglerne til en given behandling af persondata, herunder adgang til teleoplysninger. Er der tale om behandling af følsomme data, skærpes hjemmelskravet betydeligt. Desuden opstiller loven nogle grundlæggende principper, som skal efterleves, hvis persondata kan behandles (uanset om det er almindelige eller følsomme data), herunder at behandlingen skal forfølge lovlige og saglige formål (finalité-princippet) samt være proportional (dvs. ikke gå videre end formålet tilsiger). Herudover skal den registrerede have oplysning om behandlingen samt adgang til at få urigtige eller vildledende oplysninger rettet eller slettet. I forhold til teledata, dvs. oplysninger om, hvem en given person har kommunikeret med, hvornår og hvordan, er beskyttelsen - fordi der er tale om indgreb i kommunikationshemmeligheden - endnu mere vidtgående.[24] Desuden stiller persondatareglerne krav til datasikkerhed, der sikrer, at i hvert fald offentlige myndigheder og teleselskaber opretholder et forholdsvis højt sikkerhedsniveau, således at risikoen for lækager og misbrug minimeres.

Som de øvrige regler indeholder persondatalovgivningen dog en række undtagelser og vanskelige afvejningsregler, jf. nærmere nedenfor, ligesom de mange aktuelle sager om brud på datasikkerheden har vist, at reglerne langt fra altid overholdes i praksis. Hertil kommer, at reglerne naturligvis aldrig kan give fuldstændighed sikkerhed mod lækager, hvad enten disse er utilsigtede eller tilsigtede, og uanset om de består af oplysninger, der sendes ud eller udefrakommende, der trænger ind og tager oplysningerne.

Ud over de nævnte regler er der også andre regelsæt, der på mere specifikke områder tilsigter at beskytte den enkeltes ret til privatliv - og således modvirker overvågning, herunder fx sundhedslovgivningen, hvorefter patienten som klart udgangspunkt skal give et såkaldt "informeret" samtykke til både selve sygdomsbehandlingen og behandling af oplysninger om patienten.[25] Ligeledes er der i den finansielle lovgivning regler, der skal sikre, at oplysninger om kundernes finansielle forhold ikke misbruges.[26]

3.4 Sammenfatning

Der er således en meget stor mængde regler, der på forskellige niveauer og ud fra forskellige indfaldsvinkler og hensyn begrænser adgangen til at foretage overvågning, men tankegangen bag den grundlæggende ret til privatlivets fred, som alle de nævnte regler værner om, er den samme, nemlig at det enkelte menneske har krav på et frirum, en privatsfære, hvor andres indblanding ikke skal tåles, et rum for selvrealisering, hvor man kan leve sit liv efter egne ønsker og forhåbninger, og hvor man kan danne sine meninger og sin personlighed.[27] En indtrængen i dette frirum i form af overvågning, fx af en persons handlinger og bevægelsesmønster, sundhedstil-

stand, finansielle forhold eller kommunikation med omverdenen, udgør en krænkelse af den pågældendes privatliv, medmindre forholdet omfattes af en af undtagelserne til retten til privatlivsfred. Når det først er konstateret, at der foreligger en given form for overvågning - også i juridisk forstand - samler interessen sig derfor typisk om disse undtagelser, jf. straks nedenfor.

4. Undtagelser og modifikationer til retten til privatlivets fred

4.1 EMRK art. 8, stk. 2

Retten til privatlivets fred gælder ikke undtagelsesfrit. Efter EMRK art. 8, stk. 2, gælder, at *"ingen offentlig myndighed må gøre indgreb i udøvelsen af denne ret, medmindre det sker i overensstemmelse med loven og er nødvendigt i et demokratisk samfund af hensyn til den nationale sikkerhed, den offentlige tryghed eller landets økonomiske velfærd, for at forebygge uro eller forbrydelse, for at beskytte sundheden eller sædeligheden eller for at beskytte andres rettigheder og friheder"*. Idet der er tale om en undtagelsesbestemmelse, skal den fortolkes indskrænkende, ligesom behovet for overhovedet at gøre indgreb efter EMD's praksis skal godtgøres på en overbevisende måde. Også EU-charteret indeholder undtagelser til art. 7 og 8 om retten til privatlivsfred og persondatabeskyttelse, jf. art. 52, stk. 1. Disse undtagelser skal i det hele forstås i overensstemmelse med EMRK art. 8.

Den første betingelse efter EMRK art. 8, stk. 2, for, at et indgreb i privatlivets fred fra myndighedernes side er lovligt, er, at indgrebet har hjemmel (legalitetskravet). Det er dog ikke tilstrækkeligt, at der er en hjemmel (hvad der normalt er til indgreb fra myndigheders side),[28] den skal også have en vis "kvalitet", således at der en vis garanti for, at hjemmelen ikke misbruges, men kun anvendes inden for dens tilsigtede område. I kvalitetskravet ligger, at hjemlen dels skal være tilgængelig for borgerne, dels have en vis klarhed og præcision, således at det ikke er helt arbitrært, hvad retsstillingen på området er, men at man som borger selv - eventuelt med hjælp fra en advokat eller anden rådgiver med indsigt i det pågældende område - kan forudskikke denne retsstilling.

Den anden betingelse er, at indgrebet skal være "nødvendigt i et demokratisk samfund" (nødvendigheds- eller proportionalitetskriteriet). Heri ligger en proportionalitetsvurdering, dvs. at der skal være en rimelig balance mellem det formål, der søges realiseret ved det pågældende indgreb, og det middel, som indgrebet repræsenterer.[29] Idet de fleste myndighedsindgreb opfylder legalitetskravet, og idet listen af relevante samfundsmæssige hensyn, der kan begrunde et indgreb, er meget bred, jf. nedenfor, er det som regel proportionalitetsvurderingen, som interessen samler sig om: Hvordan skal afvejningen foretages mellem det formål, som indgrebet i privatlivet tjener, fx terrorbekæmpelse, og det middel, som anvendes, fx overvågning? Dette er det helt centrale spørgsmål. Ved proportionalitetsvurderingen lægger EMD generelt vægt på, om de anvendte foranstaltninger er rimelige og egnede til at opnå det anerkendelsesværdige formål.[30] Vurderingen foretages i øvrigt konkret i hver enkelt sag, hvilket i sig selv gør det vanskeligt at forudskikke retsstillingen på et givet område.

Det skal i den forbindelse bemærkes, at EMD indrømmer staterne en vis "skønsmargin" ved vurderingen af, om det er nødvendigt at gøre indgreb i privatlivets fred samt de midler, der i så fald skal bruges for at opnå det anerkendelsesværdige formål.[31] Omfanget af staternes skønsmargin varierer alt efter rettighedens karakter, indgrebets intensitet mv. I forhold til systematisk overvågning, der alt andet lige udgør et alvorligt indgreb i retten til privatlivets fred, vil staternes skønsmargin som udgangspunkt være lille - og EMD's prøvelse af indgrebet omvendt stor. Er der tale om, at indgrebet - hvad der ofte er tilfældet med overvågning - er begrundet i hensynet til beskyttelse af statens sikkerhed eller opklaring af alvorlig kriminalitet, er staternes skønsmargin normalt stor, hvilket altså trækker i den modsatte retning. Denne ubestemte og varierende karakter af staternes skønsmargin, og samspillet mellem denne og proportionalitetsvurderingen, gør det selvsagt endnu vanskeligere at forudse udfaldet af en given sag, hvorved staternes skønsmargin i sig selv kan virke som en modifikation til grundprincippet om privatlivets fred.

Endelig er det en tredje betingelse (for at gøre undtagelse efter EMRK art. 8, stk. 2), at indgrebet sker for at opfylde et af de væsentlige samfundsmæssige hensyn, der (udtømmende) er oplistet i undtagelsesbestemmelsen i art. 8, stk. 2. Disse hensyn er uhyre bredt affattet, og det er yderst sjældent, at et lovfæstet indgreb i privatlivets fred ikke opfylder denne betingelse. I forhold til digital overvågning fra

myndighedernes side, fx i form af aflytning, adgang til e-mailkommunikation, logning af teledata mv., er det navnlig hensynet til den nationale sikkerhed og kriminalitetsforebyggelse, herunder forebyggelse af terror, der påberåbes. Tankegangen bag undtagelsen i art. 8, stk. 2, er, at disse hensyn - og de øvrige i bestemmelsen oplistede hensyn - er så væsentlige i en bredere samfundsmæssig forstand, at de, hvis de øvrige betingelser (om hjemmel og proportionalitet) i øvrigt er opfyldt, kan veje tungere end den enkelte persons ret til privatliv.

Sammenfattende kan det om undtagelsen i art. 8, stk. 2, fastslås, at de tre betingelser, der skal være opfyldt, dels er meget brede, dels indebærer en konkret og ofte vanskelig afvejning af modsatrettede hensyn. Det gør bestemmelsen fleksibel og dynamisk, men samtidig svært forudsigelig - til skade for retssikkerheden. Selv om art. 8, stk. 2, som andre undtagelser generelt skal fortolkes indskrænkende, udgør den i forhold til overvågning næppe nogen skræmmende barriere for statslige overvågningstiltag. Disse har som regel et sikkert hjemmelsgrundlag for indgrebet og kan begrunde det med et eller flere anerkendelsesværdige hensyn. Tilbage står herefter kun at sikre, at de midler, der tages i anvendelse, er rimeligt afpassede og egnede i forhold til formålet, dvs. at proportionalitetsbetingelsen er opfyldt.

4.2 Straffeloven

Som udgangspunkt underbygger straffeloven værnet om privatlivets fred, men der er kun nogle få, helt bestemte fredskrænkelser, der er gjort strafbare, og straffeloven udgør derfor ikke nogen bred beskyttelse af privatlivets fred. Det er godt og nødvendigt for retssikkerheden, at straffeloven - netop fordi den giver hjemmel til straf, herunder fængsel - i videst muligt omfang er klart og præcist afgrænset, således at det er muligt for borgerne at forudse deres retsstilling.[32] Omvendt medfører den forholdsvis snævre beskyttelse, at loven ofte slet ikke vil kunne anvendes, særligt i forhold til nye og ukendte overvågningsværktøjer, der opstår i informationssamfundet. Hertil kommer, at betingelsen om, at en given handling for at være omfattet af reglerne ikke blot skal opfylde gerningsindholdet i den pågældende bestemmelse, men også være "uberettiget",[33] generelt gør reglerne vanskelige at anvende i praksis.

I betingelsen om, at indgrebet skal være uberettiget, ligger ifølge forarbejderne til bestemmelserne et ønske om at holde helt atypiske handlinger uden for det strafbare område, også selvom handlingen omfattes af gerningsbeskrivelsen i den pågældende bestemmelse.[34] [35] Det er ikke ud fra teori og praksis muligt at angive præcise anvisninger på, hvornår en handling er materielt "atypisk" og derfor kan være berettiget (og dermed ikke strafbar). Vurderingen må foretages konkret. I retspraksis er der eksempler på, at nyhedsmediernes indgreb i privatlivets fred konkret kan være berettiget - ud fra en afvejning i forhold til hensynet til informations- og ytringsfriheden.[36] Som udgangspunkt er disse regler i straffeloven endvidere undergivet privat påtale, hvilket kan gøre det praktisk svært for den krænkede at forfølge sin ret.

Hvor straffeloven vel ikke har indbyggede "undtagelser" til værnet om privatlivets fred, men nok flere eller færre "huller", rummer reglerne om politiets beføjelser i forbindelse med efterforskningen af strafbare handlinger en meget lang række tilsigtede undtagelser, jf. nærmere afsnit 5 nedenfor.

4.3 Persondataloven

Persondatalovgivningen indeholder også et betydeligt spillerum for overvågning. For det første gælder loven slet ikke for behandlinger, der udføres for politiets og forsvarets efterretningstjenester, jf. § 2, nr. 8. For det andet er der bestemmelser i loven, hvor hensynet til beskyttelsen af den enkeltes privatliv og persondata viger for større samfundsmæssige hensyn, og som derfor efter omstændighederne kan bruges som hjemmel til et givet overvågningstiltag. Det gælder særligt for offentlige myndigheder, herunder politiet, idet behandling af følsomme data bl.a. kan finde sted, hvis behandlingen er nødvendig for varetagelsen af en myndigheds opgaver, hvis behandlingen er nødvendig af hensyn til en offentlig myndigheds varetagelse af sine opgaver på det strafferetlige område, eller hvis behandlingen sker for at varetage vigtige samfundsmæssige interesser. Selv om det således bestemt er muligt for en myndighed at finde hjemmel i loven til en given behandling, sætter de grundlæggende krav til databehandlingen, der altid skal være opfyldt, herunder navnlig finalité- og proportionalitetsprincippet (jf. ovenfor), dog visse begrænsninger, der kan være betydningsfulde i forhold til et givet overvågningstiltag.

En anden ofte anvendt hjemmel, dog kun til behandling af almindelige, ikke-følsomme oplysninger, er bestemmelsen om, at behandling kan ske, hvis

behandlingen er nødvendig for, at den dataansvarlige eller den tredjemand, til hvem oplysningerne videregives, kan forfølge en berettiget interesse og hensynet til den registrerede ikke overstiger denne interesse (den såkaldte interesseafvejningsregel). Også denne bestemmelse illustrerer, at persondataloven generelt ikke er en nem lov at arbejde med, og dens mange vage og upræcise udtryk, begreber og afvejningsregler, gør bestemt ikke arbejdet nemmere, heller ikke i relation til spørgsmålet om overvågning.[37] Hvad ligger der således i ordene "nødvendigt" og "berettiget interesse" - og hvornår overstiger den berettigede interesse "klart" hensynet til den registrerede?

Også i forhold til privates mulighed for at foretage overvågning er der brugbare ventiler i persondataloven - om end ikke så mange. Indhentelse af samtykke fra den registrerede er i alle henseender en gyldig hjemmel. Kan der ikke indhentes samtykke (hvad der ofte er tilfældet), kan hjemlen efter omstændighederne findes i andre bestemmelser, navnlig interesseafvejningsreglen, jf. lige ovenfor. Som beskrevet rejser denne bestemmelse flere fortolkningsspørgsmål.

5. Særligt om overvågning inden for det strafferetlige område

5.1 Kriminalitetsbekæmpelse og politiets hjemmel til overvågning

Hensynet til en effektiv kriminalitetsbekæmpelse er et af de hovedhensyn, der hjemler en undtagelse fra bl.a. retten til privatliv, retten til beskyttelse af persondata og retten til fri kommunikation. Spørgsmålet er ikke, om dette er rimeligt. Det er en undtagelse, der ikke blot møder forståelse, men som vel nærmest er et samfundsmæssigt krav: Grundrettighederne skal selvsagt ikke være så ufravigelige, at enhver kriminel skal kunne krybe i skjul bag disse og undgå at blive afsløret og pågrebet. På den anden side anvendes disse indgreb, før vi ved, hvem der er kriminel. Det er således i efterforskningsfasen, politiet har brug for at kunne foretage rumaflytninger, telefonaflytninger, dataindsamling mv. Det, der kendetegner efterforskning, er dels, at den retter sig mod en eller flere mistænkte, som politiet "formoder" er gerningsmænd, dels at den let kan udsætte andre, som end ikke er genstand for mistanke, for at få krænket privatliv mv. Tilfældige besøgende i det rumaflyttede hjem og elektroniske eller telefoniske samtalepartnere bliver optaget på det samme medie, som den efterforskede og mistænkte - men altså endnu præsumptivt uskyldige.

Reglerne for, hvornår politiet må anvende tvangsindgreb[38] (anholdelse, aflytning, dataaflæsning, afbrydelse af radio- og telekommunikation m.v.) tager alle afsæt i, at der er mistanke om, at en bestemt forbrydelse er begået eller tilsigtes begået, og ud fra dette grundkriterium hjemles mere og mere vidtgående indgreb i borgernes privatliv i takt med alvoren og grovheden af den forbrydelse, der efterforskes/søges forebygget. Reglerne har således indbygget en proportionalitet, der sikrer, at de alvorligste indgreb i borgernes privatliv alene sker, hvor der er en tungtvejende grund i form af en konkret, alvorlig forbrydelse som omdrejningspunktet. For at sikre, at denne proportionalitet efterleves, er der endvidere krav om, at indgrebene kun må finde sted i henhold til en kendelse, der afsiges af en dommer. Den part, indgrebet vedrører, vil være repræsenteret af en advokat, men parten selv (den aflyttede) får i sagens natur ikke underretning om hverken rettens beslutning eller indgrebets foretagelse. Medmindre det vil skade efterforskningen, røbe fortrolige oplysninger om politiets efterforskningsmetoder eller lignende, skal den aflyttede imidlertid efterfølgende gives underretning om det foretagne indgreb.[39]

Til yderligere sikring af proportionaliteten er der foreskrevet sletning af de indhentede oplysninger, hvis de ikke har efterforskningsmæssig betydning,[40] ligesom oplysninger vedrørende andre forbrydelser (end den, der har dannet baggrund for tilladelsen til indgrebet), som politiet får kendskab til gennem aflytningen (såkaldte tilfældighedsfund) nok kan bruges til efterforskning, men må som hovedregel ikke anvendes som bevis i retten. Dette sidste gælder dog ikke, hvis tilfældighedsfundet vedrører forbrydelser af en sådan grovhed, at de også selv kunne danne baggrund for det foretagne indgreb.[41]

Overvågning foretaget af politiet i forbindelse med en strafferetlig efterforskning kan have karakter af observation, hvor en politiassistent rent fysisk holder øje med den eller de pågældende personer. Sådan skygning kræver ikke hjemmel og er ikke reguleret i retsplejeloven. Det er derimod overvågning af personer, der befinder sig inde i private rum i form af løbende aflytning eventuelt suppleret af videoovervågning.[42] Her er kravene[43] bl.a., *at* der skal være "bestemte grunde til at antage" at denne metode

kan skaffe beviser i sagen, *at* indgrebet skal være af "afgørende betydning for efterforskningen", *at* det skal være tale om efterforskning af en forbrydelse, der enten har en strafferamme på fængsel i 6 år eller derover eller er af en nærmere bestemt beskaffenhed, herunder terrorisme mv., og *at* lovovertrædelsen skal have medført eller "kan medføre fare for menneskers liv eller velfærd eller for betydelige samfundsværdier".

For så vidt angår efterforskningskridt vedrørende konkrete mistanker om forbrydelser, der enten er begået eller søges begået, der involverer informations- og kommunikationsteknologi, kan følgende muligheder oplistes:

1. Aflytning af telefonsamtaler uanset teknologi (telefonaflytning),
2. Rumaflytning. Dette vil typisk ske ved opsat lytteudstyr, men kan også ske via mobiltelefoner eller computeres mikrofoner.
3. Teleoplysning. Det vil sige hvilke apparater, der er eller har været i forbindelse med hvilke
4. Udvidet teleoplysning. Det vil sige hvilke apparater, der indenfor et bestemt, nærmere angivet område sættes eller har været sat i forbindelse med hinanden.
5. Hastesikring af elektroniske data. Politiet kan meddele udbydere af telenet eller teletjenester pålæg om at foretage hastesikring af elektroniske data, herunder trafikdata. Pålægget kan kun omfatte data, der er nødvendige for en given efterforskning og sikringsperioden kan ikke overstige 90 dage.
6. Dataaflæsning. Dette omfatter aflæsning af "ikke offentligt tilgængelige oplysninger" i et informationssystem "ved hjælp af programmer eller andet udstyr"
7. Observation. Dette kan, som nævnt også ske ved hjælp af computere m.v. og må også omfatte optagelse/overvågning på ikke-frit tilgængelige steder. Dette omfatter (efter lidt forskelige krav fordi indgrebet er mere eller mindre indgribende) ikke blot haver, carporte, altaner m.v. men også beboelsesrum og virksomhedslokaler af enhver art.

Alle de nævnte indgreb har det tilfælles, at de er reguleret i retsplejeloven og at de kan tillades ud fra en afvejning af indgrebets intensitet og den konkrete forbrydelse, der efterforskes. Det er således muligt for retten at foretage en konkret proportionalitetsvurdering mellem hensynet til privatlivets fred og behovet for at efterforske og forhindre konkrete forbrydelser.

Derudover er der imidlertid andre overvågningsredskaber til brug for politiet. Det er således tilladt - og ikke direkte reguleret[44] - for politiet at foretage tv-overvågning af offentlig vej, gade og plads. En sådan overvågning har mindst tre formål. Det ene formål er, at de opsatte overvågningskameraer skal virke præventive. Det andet formål er, at de kan give politiet mulighed for at gribe ind overfor igangværende kriminalitet, hvis de monitoreres, og det tredje formål er at gemme optagelserne, således at de kan fremfindes, hvis der senere anmeldes eller på anden måde opstår mistanke om kriminalitet i det pågældende område.

Det sidstnævnte formål - at opsamle data blot for at have dem, såfremt der efterforskningsmæssigt skulle blive brug for dem - er det formål, der alene bærer reglen i retsplejelovens § 786, stk. 4. hvorefter udbydere af telenet eller teletjenester pålægges "at foretage registrering og opbevaring i 1 år af oplysninger om teletrafik til brug for efterforskning og retsforfølgning af strafbare forhold". Det er med hjemmel i denne bestemmelse, at den såkaldte "logningsbekendtgørelse" er udstedt.[45] Kendetegnende for den logning (dvs. registrering), der er omfattet af bekendtgørelsen er, at den ikke finder sted ud fra en konkret formodning om, at der er ved at blive begået eller er begået en forbrydelse, men at indsamlingen foregår blandt alle borgere. De, der udsættes for denne overvågning er for langt det overvejende flertals vedkommende hverken ved at begå noget kriminelt eller planlægger at begå noget kriminelt - og slet ikke kriminalitet af en type, der normalt vil kunne give adgang til at gennemføre målrettede, konkrete tvangsindgreb. Ved alle fastnet- og mobiltelefonsamtaler (herunder SMS-, ENS- og MMS-kommunikation) skal det således registreres hvilket nummer, der har kaldt op og hvilket nummer, der er kaldt op til, samt hvilke mobilmaster man er koblet på med henholdsvis start- og sluttidspunkt.[46]

Denne form for overvågning, hvor personlige og beskyttede oplysninger indsamles alene med det formål at have dem til senere brug, hvis det skulle vise sig nødvendigt, er således væsensforskellig fra den normale informationsindsamling, der foregår i forbin-

delse med opklaring af forbrydelser. Det var blandt andet en sådan kritikløs indsamling af oplysninger, der dannede baggrund for EU-domstolens afgørelse af 8. april 2014.[47] Sagerne handlede om gyldigheden af EU's logningsdirektiv,[48] og domstolen fandt efter en udførlig gennemgang af direktivet, de bagvedliggende hensyn og de krav, direktivet stillede sammenholdt med EU-charterets artikler 7,8 og 52, stk. 1, at direktivet var i strid med EU-retten og derfor var ugyldigt. Baggrunden for ugyldigheden var, at direktivet havde "overskredet de grænser, som overholdelsen af proportionalitetsprincippet kræver…". Der var tale om en lang række betragtninger, der samlet set førte til denne vurdering, og det er derfor vanskeligt at udnævne en eller flere af disse betragtninger, som den "afgørende" for resultatet.

Justitsministeriet har efterfølgende offentliggjort en vurdering[49] af i hvilket omfang den daværende danske logningsbekendtgørelse kunne opretholdes efter domstolens afgørelse. Ifølge denne vurdering var den daværende bekendtgørelse ikke i strid med EU-reglerne[50], men ministeriet nåede frem til denne konklusion primært ud fra en argumentation om, at man fra politiets side kun kunne få adgang til at se/bruge oplysningerne, hvis reglerne om tvangsindgreb i retsplejeloven var opfyldt. Notatet er imidlertid påfaldende tavst om betydningen af den kritikløse og altomfattende indsamling af dataene på trods af, at denne indsamlingsproces er en del af de betragtninger, der førte frem til EU-Domstolens konklusion.[51] Domstolen bemærker[52] bl.a. at den altomfattende registrering *"... indebærer ... et indgreb i de grundlæggende rettigheder for praktisk talt hele den europæiske befolkning."*

Dette ønske om at indsamle data om samtlige borgeres telefoniadfærd mv. kunne med lige så stor ret tilsige, at samtlige borgere ved fødslen afleverede fingeraftryk, DNA, Iris-identifikationsoplysninger m.v., fordi alle sådanne oplysninger om borgerne kunne være praktiske at have ved hånden i forbindelse med en efterforskning. Det samme vil indsamlede GPS-oplysninger om fx vore bilers bevægelser være. Der er dog - udover spørgsmålet om proportionalitet - mindst tre problemstillinger knyttet hertil: 1) Betingelserne for at politiet skal have adgang til oplysningerne, 2) risikoen for, at oplysningerne tilgås og anvendes af uvedkommende, og 3) hvad bevidstheden om overvågningens tilstedeværelse og udbredthed måtte have på borgernes (lovlige) adfærd. Hertil kan endelige føjes problemstillingen om udveksling af de oplysninger, som politiet kan få adgang til, med andre offentlige nationale og/eller internationale myndigheder.

5.2 Efterretningsvirksomhed mv. og efterretningstjenesters hjemmel til overvågning

De i forrige afsnit beskrevne regler og krav vedrørende tvangsindgreb mv. overfor borgerne gælder ikke blot det almindelige politi, men også politiets efterretningstjeneste (PET). Dette gælder imidlertid kun den del af PET's virksomhed, der indebærer egentlige tvangsindgreb over for borgerne i forbindelse med efterforskning og forfølgning af den type kriminalitet, som hører under PET's område. Herudover har PET således en næsten ubegrænset adgang til at igangsætte undersøgelser af personer, "hvis undersøgelserne må antages at have betydning for varetagelsen af tjenestens opgaver vedrørende forebyggelse og efterforskning af overtrædelser af straffelovens kapitel 12 og 13 eller er nødvendige til varetagelsen af tjenestens øvrige opgaver".[54]

Tjenesten må ikke anvende tvangsindgreb direkte overfor borgerne (medmindre betingelserne i retsplejeloven er opfyldt), men har adgang til at kræve alle typer af oplysninger fra andre forvaltningsmyndigheder, hvis oplysningerne "må antages at have betydning for varetagelsen af tjenestens opgaver vedrørende forebyggelse og efterforskning af overtrædelser af straffelovens kapitel 12 og 13."[55] [56] Endelig er der (så godt som) fri adgang til gnidningsfri udveksling af oplysninger mellem Forsvarets og Politiets efterretningstjenester.[57]

Forsvarets Efterretningstjeneste (FE) er nærmere reguleret i lov om Forsvarets Efterretningstjeneste, hvis virksomhed, jf. lovens § 1, er rettet mod forhold i udlandet, der har interesse for beskyttelsen af danske interesser i nærmere beskrevet omfang. Også FE må indsamle information, der "kan have betydning" for tjenestens virksomhed.[58] Indsamling af information om personer, der er hjemmehørende i Danmark, er dog en opgave for PET, medmindre der er tale om såkaldte "tilfældighedsfund", hvor FE i forbindelse med sin virksomhed "falder over" information vedrørende sådanne personer.

Som nævnt kan FE og PET stort set frit udveksle oplysninger, blot det "kan have betydning" for en af de to tjenesters opgave.[59] Endvidere kan FE videregive

oplysninger til bl.a. udenlandske myndigheder og tjenester, herunder også personoplysninger, blot oplysningerne enten kan "antages at have betydning for tjenestens opgaver"[60] eller - for så vidt angår følsomme oplysninger - bl.a. hvis undtagelserne i persondataloven, jf. ovenfor under afsnit 4.3, er opfyldt.

Endelig skal Center for Cybersikkerhed nævnes. Dette center er en del af FE, men er selvstændigt lovreguleret[61] og har til opgave at "understøtte et højt informationssikkerhedsniveau i den informations- og kommunikationsteknologiske infrastruktur, som samfundsvigtige funktioner er afhængige af", som det siges i lovens § 1. Centerets netsikkerhedstjeneste kan uden retskendelse behandle trafik- og pakkedata med henblik på at kunne understøtte et højt informationssikkerhedsniveau, som det siges i loven.[62] Pakkedata er selve indholdet af kommunikation, der transmitteres gennem digitale netværk eller tjenester, hvor trafikdata er data, der behandles med henblik på at transmittere pakkedata. Denne tjeneste har således adgang til at læse indholdet af enhver form for kommunikation, der foretages bl.a. via internettet med det klare formål at undgå forskellige former for angreb på datasystemer hos det offentlige eller i (større) private virksomheder, der tilslutter sig centeret.

For at regulere tjenestens adgang til disse data, foreskriver loven[63] bl.a., at "indsamling af personoplysninger skal ske til udtrykkeligt angivne og saglige formål, og senere behandling må ikke være uforenelig med disse formål". Loven angiver endvidere de formål, der skal varetages, for at tjenesten kan behandle personoplysninger, men disse formål er for en dels vedkommende ganske skønsprægede og vanskelige at konkretisere. Se f.eks. lovens § 10, nr. 6: "behandlingen er nødvendig for, at Center for Cybersikkerhed eller den tredjemand, til hvem oplysningerne videregives, kan forfølge en berettiget interesse, og hensynet til den pågældende person ikke overstiger denne interesse"

Såvel en del af PET's virksomhed som en stor del af FE's virksomhed, herunder Center for Cybersikkerheds virksomhed, er til forskel fra den konkrete efterforskning af forbrydelser rettet mod forebyggelse og forhindring af fremtidige forbrydelser og trusler. Dette er i sig selv prisværdigt og yderst samfundsgavnligt. Samtidig vanskeliggør det imidlertid en meget skarp proportionalitetsvurdering, fordi det onde, der søges undgået, meget ofte vil være uhyre ukonkret, vanskeligt beviseligt og ofte på så tidlige forstadier, at der end ikke er tale om strafbart forsøg.

PET og Center for Cybersikkerhed er underlagt et tilsyn, der af egen drift eller efter klage overholder en del af reglerne for deres virksomhed, herunder behandling af personoplysninger.[64] Tilsynet kan i den forbindelse afgive udtalelser over for PET henholdsvis over for Center for Cybersikkerhed, og følger disse organer ikke udtalelserne, skal der ske indberetning herom til henholdsvis justits- og forsvarsministeren. Tilsynet er uafhængigt og dets afgørelser kan ikke indbringes for anden administrativ myndighed. Tilsynet er underlagt Folketingets Ombudsmands kompetence og dets afgørelser kan indbringes for domstolene jf. grundlovens § 63. Medlemmerne af tilsynet udpeges af justitsministeren og dets formand skal være landsdommer.

6. Retspraksis vedrørende overvågning

6.1 Praksis fra EMD

Menneskerettighedsdomstolen har afsagt en række domme, der direkte eller indirekte vedrører overvågning, og som bidrager til at præcisere anvendelsesområdet og indholdet af art. 8 om retten privatlivets fred, herunder rækkevidden af undtagelsen i art. 8, stk. 2. Det ligger uden for formålet med denne artikel at gå dybere ind i en analyse af de enkelte domme, og en række af de vigtigste domme er direkte eller indirekte omtalt i afsnittene om EMRK art. 8 ovenfor. Nogle få, men væsentlige træk fra retspraksis skal dog fremhæves her.

For det første har EMD fastslået, at selve det, at en offentlig myndighed systematisk indsamler og opbevarer oplysninger om personers privatliv, i sig selv er tilstrækkeligt til at aktualisere privatlivsbeskyttelsen og dermed gøre art. 8 anvendelig.[65] Hvorvidt de pågældende oplysninger rent faktisk efterfølgende bliver anvendt (og til hvad og hvor længe), er i den henseende ikke afgørende.[66] Selv om anvendelsesområdet for art. 8 som nævnt er bredt, er det dog - som også anført ovenfor - ikke enhver personoplysning, der udgør et indgreb i privatlivets fred efter art. 8, stk. 1. EMRK art. 8 har således et snævrere anvendelsesområde end persondataloven. Hvorvidt en given personoplysning falder ind under privatlivets fred i art. 8, vurderer EMD i den konkrete sag under hensyntagen til den kontekst, hvori oplysningerne er

blevet indsamlet og opbevaret, optegnelsernes karakter, den måde hvorpå de anvendes og behandles samt de resultater, der herved opnås.[67]

Politiets opbevaring af DNA-profiler, vævsprøver og fingeraftryk fandtes på den baggrund at udgøre et indgreb. De logningsdata, der i medfør af logningsbekendtgørelsen indsamles og registreres om danskernes elektroniske kommunikation (hvem har kommunikeret med hvem, hvordan og på hvilke tidspunkter) er ligeledes persondata, der - idet de vedrører kommunikationshemmeligheden (korrespondance), der er særskilt fremhævet under art. 8 - udgør et indgreb efter art. 8, stk. 1 (og som derfor skal opfylde betingelserne i art. 8, stk. 2, for at kunne retfærdiggøres). Se om logningsreglerne nærmere ovenfor afsnit 5.1.

Udgør den pågældende form for overvågning et indgreb efter art. 8, stk. 1, opstår spørgsmålet, om indgrebet opfylder betingelserne for at kunne undtages efter art. 8, stk. 2. Betingelserne er gennemgået ovenfor. I relation til legalitetskravet følger det af praksis fra EMD, at der dels skal være hjemmel til indgrebet, dels at den pågældende hjemmel skal være klar og præcis, således at retstillingen er forudsigelig for borgeren og hjemlen ikke kan misbruges af myndighederne til at lave vilkårlige indgreb.[68] Bliver det pågældende indgreb begrundet med hensynet til statens sikkerhed - hvad der er typisk i forbindelse med overvågningsforanstaltninger, fx fra efterretningstjenesternes side - gælder hjemmelskravet stadig, men EMD accepterer, at det er knap så præcist som på andre områder, idet trusler mod statens sikkerhed kan være vanskeligt at afgrænse præcist. Reglerne kan derfor godt være vagt formulerede og lægge op til skønsmæssige afgørelser. Til gengæld stiller EMD i denne situation - for at råde bod på den forøgede risiko for, at reglerne misbruges - et skærpet krav om processuel beskyttelse, bl.a. i form af skærpede krav til afgørelsens begrundelse og underretningspligten over for borgerne, samt at indgrebet skal kunne prøves ved et uafhængigt og upartisk organ med kompetence til at vurdere alle relevante faktiske og retlige spørgsmål under en procedure med kontradiktionsadgang.[69]

Ved proportionalitetsvurderingen lægger EMD som tidligere nævnt vægt på, om indgrebet er rimeligt og egnet til at opnå de anerkendelsesværdige mål. I øvrigt anlægges en samlet, konkret helhedsvurdering, hvor der også tages hensyn til staternes skønsmargin, hvilket gør det vanskeligt at forudsige retsstillingen i konkrete sager. I forhold til overvågning indikerer den foreliggende praksis dog, at EMD lægger betydelig vægt på, om der er tale om generel og forskelsløs masseovervågning uden nærmere hensyn til hverken karakteren eller alvorligheden af den eller de forbrydelser, som overvågningen skal forhindre, eller om de overvågne personer overhovedet har eller kan have noget med de pågældende forbrydelser at gøre. I så fald er domstolen tilbøjelig til at anse art. 8 for overtrådt.[70] Som beskrevet ovenfor anvender EU-Domstolen anvender lignende betragtninger i dommen om logningsdirektivet.

I forhold til de relevante hensyn, som skal foreligge, for at et indgreb kan lovliggøres efter art. 8, stk. 2, viser EMD's praksis, at hensynet til statens og borgernes sikkerhed og kriminalitetsbekæmpelse selvsagt har betydelig, men langt fra ubegrænset vægt, idet kravene til legalitet og proportionalitet fortsat er til stede, om end de kan slækkes afhængig af det pågældende indgrebs nærmere karakter.

Sammenfattende må det konstateres, at det vel er muligt på baggrund af den foreliggende praksis at opstille visse kriterier for, hvad der nærmere ligger i undtagelsen i EMRK art. 8, stk. 2, men at disse kriterier langt fra er klare, da vurderingen i høj grad er skønsmæssig og afhænger af det konkrete indgreb. Praksis viser også, at der er et betydeligt - men langt fra ubegrænset - spillerum for staterne i forhold til indgreb, der er begrundet i hensynet til statens sikkerhed.

6.2 Praksis fra EU-Domstolen

Den helt centrale dom fra EU-Domstolen er dommen vedrørende underkendelsen af logningsdirektivet. Dommen er behandlet ovenfor i afsnit 5.1.

6.3 National praksis

Danske domstole og Datatilsynet, der fører tilsyn med persondataloven, har foreløbig kun en beskeden praksis vedrørende overvågning. De foreliggende sager begrænser sig så vidt ses primært til spørgsmål om tv-overvågning (som nu er lovreguleret), nyhedsmediers brug af skjult kamera og overvågning af kendte mennesker (hvilket rejser nogle medieretlige spørgsmål om ytringsfrihed mv., som ikke skal forfølges nærmere her) samt arbejdsgiveres overvågning af medarbejdernes e-mail- og internetkommuni-

kation. I relation til sidstnævnte er retsstillingen efter praksis i grove træk, at arbejdsgiveren, forudsat den ansatte informeres på forhånd, kan overvåge den ansattes internetforbrug og læse den ansattes mail, dog ikke private, ikke-arbejdsrelaterede mails, idet disse er omfattet af brevhemmeligheden i straffelovens § 263, stk. 1.[71] Retsstillingen afspejler således også på dette område den afvejning, der typisk må foretages mellem hensynet til den enkeltes ret til privatliv over for andre væsentlige hensyn, her arbejdsgiverens ledelsesret og ret til at føre en vis form for kontrol med den ansattes handlinger i arbejdstiden.

I forhold til IT-overvågning og internettet foreligger der nogle få domstolsafgørelser vedrørende enkeltstående tilfælde af fx hacking og industrispionage, men endnu ingen afgørelser vedrørende overvågning i nærværende artikels forstand, dvs. en mere systematisk og vedvarende kontrol med andre. Det igangværende retsopgør i kølvandet på Se & Hør-skandalen vil dog antageligt ændre herpå, ligesom der næppe er tvivl om, at den stigende overvågning (fra både det offentlige og privates side), der finder sted via internettet, herunder sociale medier og tjenester, vil resultere i sager ved Datatilsynet og domstolene.

7. Overvågning udført af andre myndigheder end politi og efterretningsvæsen

Det er ikke kun politiet og efterretningstjenesterne, der kan have en interesse i at foretage forskellige former for overvågning af borgerne. Særligt har det givet anledning til offentlig debat, at SKAT i en periode havde en praksis, hvor de - uden retskendelse - anmodede teleudbydere om at få udleveret såkaldte teledata, dvs. oplysninger om privatpersoners kommunikation via telefon, internet og andre telekommunikationsmidler. Disse oplysninger var, hævdede SKAT, væsentlige for SKATs mulighed for at foretage korrekt skatteligning, idet teleoplysninger kan belyse, hvor en given person har opholdt sig på et givet tidspunkt, og hvem vedkommende har korresponderet med, hvilke oplysninger kan bruges til at fastslå, hvor den pågældende er skattepligtig. Hjemmelen til at kræve teledata udleveret fra teleselskaberne fandt SKAT i skattekontrollovens § 8 d, der kortfattet fastslår, at SKAT af enhver kan kræve sådanne oplysninger, der "skønnes at være af væsentlig betydning for skatteligningen".

Spørgsmålet er, om denne uhyre brede hjemmel til at kræve oplysninger, der udgør et indgreb i kommunikationshemmeligheden - og dermed privatlivets fred - er i overensstemmelse med EMRK art. 8 og de regler i EU-retten, der ligeledes værner om retten til privatlivets fred. I forhold til EU-retten er spørgsmålet komplekst og skal ikke behandles indgående her. Blot skal det konstateres, at det er usikkert, hvorvidt SKAT i forhold til EU's persondatadirektiver må kræve teledata udleveret fra teleselskaberne. Disse data må - fordi de udgør et indgreb i kommunikationshemmeligheden - som udgangspunkt slet ikke videregives, medmindre der foreligger nogle særligt væsentlige samfundsmæssige hensyn, herunder til statens sikkerhed eller kriminalitetsbekæmpelse.[72]

Hvorvidt skattemæssige hensyn også udgør et hensyn, der kan begrunde at oplysningerne må videregives, er ikke afklaret, men det er næppe tilfældet.[73] I samme retning trækker EU-Domstolens dom vedrørende logningsdirektivet, hvor Domstolen som en del af kritikken mod direktivet fremhæver, at det ikke udtrykkeligt foreskriver, adgangen til og den efterfølgende anvendelse af logningsdataene "skal være strengt begrænset til forebyggelse og afsløring af præcist afgrænsede strafbare handlinger eller strafferetlig forfølgning vedrørende sådanne".[74]

Spørgsmålet er derudover, om SKATs praksis efter skattekontrollovens § 8 d er i overensstemmelse med EMRK art. 8. Dette er ligeledes næppe tilfældet. Som beskrevet udgør indgreb i kommunikationshemmeligheden i form af registrering og behandling af teledata også et indgreb efter EMRK art. 8, stk. 1. Og allerede fordi hjemmelen, skattekontrollovens § 8 d, ikke kan siges at have den klarhed, præcision og garanti mod misbrug, som kræves efter EMD's praksis, jf. i det hele ovenfor, kan indgrebet sandsynligvis ikke undtages efter EMRK art. 8, stk. 2.[75]

Det er helt normalt i tilsynslovgivning at have hjemler svarende til skattekontrollovens § 8 d. Se f.eks. lov om finansiel virksomhed § 347, stk. 4: *"Finanstilsynet kan kræve alle oplysninger, herunder regnskaber og regnskabsmateriale, udskrift af bøger, andre forretningspapirer og elektronisk lagrede data, som skønnes nødvendige for Finanstilsynets virksomhed"* Eller selskabslovens § 17: *"Erhvervs- og Selskabsstyrelsen kan forlange de oplysninger, som er nødvendige, for at der kan tages stilling til, om loven, regler fastsat i medfør af loven og kapitalsel-*

skabets vedtægter er overholdt, herunder at kapitalgrundlaget er til stede"

Der er således en grundlæggende konflikt mellem på den ene side hensynet til myndighedernes mulighed for at varetage deres samfundsmæssige opgaver, og på den anden side den enkelte borgers krav på beskyttelse af sit privatliv og sine persondata. Som nævnt står den meget brede og upræcise formulering af skattekontrollovens § 8 d formentlig i vejen for, at bestemmelsen i sin nuværende skikkelse kan anvendes som grundlag for at indhente teledata. Men dette problem kan forholdsvis let løses ved en lovændring, der præciserer bestemmelsen, så den opfylder kravene til lovkvalitet efter EMRK art. 8. Hvis man samtidig i lovbemærkningerne sikrer sig, at også kravene vedrørende proportionalitet og relevante hensyn er opfyldt, udgør EMRK art. 8 ikke nogen væsentlig barriere for at gennemføre overvågningsmæssige tiltag. Det gælder i relation til skattekontrolloven såvel som love på andre samfundsområder. I så fald er problemstillingen mere af retspolitisk karakter. Selv om lovgiver således muligvis kan komme omkring EMRK art. 8, kan EU-retten dog stadig udgøre en barriere, jf. omtalen af logningsdommen ovenfor.

8. Privates adgang til at foretage overvågning

8.1 Overvågning som en pligt

I visse tilfælde udøver staten ikke selv overvågning, men pålægger i stedet private foretagender at gøre dette på statens vegne. Denne udvidede form for statslig overvågning er særligt blevet anvendt i den terrorlovgivning, der fulgte i kølvandet på terrorangrebet på USA d. 11. september 2001. De ovenfor behandlede logningsregler, der pålægger teleudbyderne en meget udstrakt pligt til at registrere teleoplysninger, således at politiet kan få adgang til disse til brug for efterforskning og opklaring af kriminalitet, er et illustrativt eksempel herpå. Teleloven har i øvrigt i en længere årrække pålagt teleudbydere at bistå politiet med den rent praktiske gennemførelse af de indgreb i meddelelseshemmeligheden, som er hjemlet i retsplejelovens kap. 71 og 74[76]. Her foretages selve overvågningen - den systematiske registrering af oplysninger om bestemte borgeres kommunikation - ligeledes af teleudbyderne med det formål at videregive oplysningerne til politiet.

Pligten for teleudbyderne til at bistå politiet blev skærpet med terrorpakke II i 2006, hvor der også - til brug for politiets bekæmpelse af terror - indførtes pligt for luftfartsselskaber til at foretage registrering og opbevaring i 1 år af oplysninger om passagerer og besætningsmedlemmer på luftfartøjer, der ankommer til eller afgår fra Danmark.[77] Ligeledes blev der efter hvidvaskningsloven indført pligt for bl.a. finansielle virksomheder til at "være opmærksom" på deres kunders aktiviteter, der kan have tilknytning til hvidvask eller finansiering af terrorisme, og efter omstændighederne videregive oplysninger herom til SØK.[78]

9.2 Overvågning som en ret

Grundlovens § 72 om beskyttelse af privatlivet og kommunikationshemmeligheden beskytter kun borgerne i forhold til myndighederne - ikke i forhold til andre borgere. Overvåger en virksomhed, fx en udbyder af en e-mailtjeneste, således sine brugere ved at "læse med" på e-mailkommunikationen, er § 72 ikke anvendelig på forholdet. EMRK beskytter ligeledes hovedsagelig mod myndigheders indblanding (det vertikale forhold), ikke forholdet mellem borgerne indbyrdes (det horisontale forhold). Staten har dog i et vist omfang også pligt til at sikre borgerne over for hinanden indbyrdes i forhold til udøvelse af visse af rettighederne efter konventionen, herunder særligt art. 8.[79] Det er ikke afklaret, hvor langt statens positive forpligtelser præcist rækker, men i en tvist mellem to private vedrørende den ene parts overvågning af den anden, må domstolen - som statslig myndighed - i det mindste fortolke de relevante danske retsregler i lyset af EMRK art. 8. Tilsvarende gælder for EU-charterets art. 7 og 8, hvis det er inden for et område, hvor der i øvrigt er EU-regulering, jf. ovenfor.[80]

I tilfælde, hvor private overvåger andre private, er det herefter primært de ovenfor omtalte regler i straffeloven og persondataloven, der finder anvendelse. Hvor staten som omtalt normalt har et hjemmelsgrundlag for overvågningen og kan henvise til, at overvågningen sker for at tilgodese et eller flere relevante samfundsmæssige hensyn, er dette ikke tilfældet for private. Privates overvågning må derfor formodes generelt at være ulovlig. Så enkelt er det imidlertid langt fra altid, idet de undtagelser, der gælder til straffe- og persondatalovgivningen, også kan være relevante i forholdet mellem private.

I førnævnte eksempel med e-mailudbyderen, der overvåger indholdet af brugernes private e-mailkommunikation er dette som klart udgangspunkt et

indgreb i brugernes kommunikationshemmelighed i strid med straffelovens § 263, stk. 1, nr. 1. Som nævnt omfatter straffelovens bestemmelser om fredskrænkelser imidlertid kun "uberettigede" overtrædelser, og spørgsmålet er derfor, om det pågældende indgreb er uberettiget. Her må man foretage en nærmere vurdering af indgrebet, herunder dets baggrund og intensitet. Antages det, at førnævnte e-mailudbyder overvåger brugernes e-mailkommunikation alene med det formål at undgå, at e-mailkontoen misbruges af brugerne til at distribuere børneporno, vil dette være relevant at inddrage i vurderingen, idet distribution af børneporno er strafbart, og hensynet til kriminalitetsbekæmpelse er et hensyn, der omfattes af EMRK art. 8, stk. 2.[81] E-mailudbyderen kan måske supplerende henvise til, at overvågningen af e-mailkommunikationen med henblik på bekæmpelse af børneporno også sker for at undgå, at e-mailudbyderen ifalder medvirkensansvar for distribution af børneporno, og - mere generelt - at undgå at udbyderens tjeneste forbindes med distribution af børneporno.

Også den proportionalitetsvurdering, der er så central i relation til EMRK art. 8, vil kunne spille ind. En generel overvågning af brugernes e-mailkommunikation alene for "at se, hvad der måtte dukke op" af mulige strafbare aktiviteter, er selvsagt ikke proportionalt overhovedet. Overvågningen må skulle begrænses til det mindst mulige i forhold til det mål, der forfølges. I herværende eksempel kan det ikke udelukkes, at e-mailudbyderen kan opfylde proportionalitetskravet ved at henvise til, at overvågningen alene er begrænset til identifikation af børnepornomateriale, at den sker rent maskinelt, dvs. uden menneskelig indblanding, og at såfremt der dukker relevant børnepornografisk materiale op, bliver sagen straks overgivet til politiet, hvorefter materialet bliver slettet hos tjenesteudbyderen.

I øvrigt er straffelovens regler om fredskrænkelser slet ikke anvendelige, hvis brugeren har givet samtykke til indgrebet. Idet der i eksemplet foreligger et privat aftaleforhold mellem parterne (e-mailudbyderen og -brugeren), vil hjemmelen til indgrebet muligvis også kunne findes i parternes aftale, typisk som et standardvilkår i udbyderens aftalevilkår, der berettiger udbyderen til at foretage den pågældende form for overvågning. Spørgsmålet er så, om et sådant vilkår overhovedet kan anses for gyldigt, idet det i almindelighed gælder, at vilkår i en standardkontrakt, der er særligt bebyrdende for den anden part, skal være behørigt fremhævet og i øvrigt ikke må være urimeligt, jf. aftalelovens § 36 og almindelige aftaleretlige principper. Afgørelsen heraf må selvsagt bero på en konkret vurdering, men eksemplet viser, at der i private retsforhold, hvor der typisk ligger et aftaleforhold mellem parterne, også må skeles til karakteren og det nærmere indhold af aftalen.

På det horisontale niveau er de almindelige persondatadirektiver - og andre relevante direktiver - af betydning for privates overvågning af hinanden, jf. *promusica*-sagen[82] ift. teledata, hvor EU-Domstolen udtalte, at EU-retten, herunder persondatadirektiverne, ikke er til hinder for, at medlemsstaterne i national lovgivning indfører regler, hvorefter teleudbydere er forpligtede til at udlevere teledata til private til brug for retsforfølgning, fx hvor indehavere af ophavsrettigheder får krænket deres rettigheder og har brug for de pågældende teledata (fx et navn knyttet til en IP-adresse) til at identificere krænkerne og anlægge retssag mod disse. Sådanne regler skal dog respektere de grundlæggende EU-principper, herunder om proportionalitet, hvoraf må følge, at det vil være i strid med EU-retten at pålægge nationale teleselskaber en generel og ubegrænset pligt til at udlevere teledata om deres abonnenter. Der skal foreligge en konkret og saglig anledning, og der må ikke udleveres flere data end formålet tilsiger.

I forhold til persondataloven vil overvågning, fx via digitale medier, i reglen altid indebære behandling af persondata (og ofte følsomme data), hvilket ikke blot skal have et hjemmelsmæssigt grundlag i persondataloven (fx at det sker med samtykke eller er nødvendigt for at fastlægge et retskrav), men også skal opfylde en række grundprincipper, herunder at behandlingen skal forfølge et sagligt formål og være proportionalt. Ydermere nyder den registrerede en række rettigheder, som skal respekteres, herunder krav på oplysning om, at der registreres data om den pågældende, samt ret til indsigt i, hvilke oplysninger der behandles og til hvilke formål.

De forholdsvis strenge krav i persondataloven gør det som udgangspunkt vanskeligt for private at legitimere overvågning af andre private, særligt hvis der er tale om mere massiv og "automatisk" overvågning, fx via digitale medier og tjenester. På den anden side indeholder loven som anført oven for mange undtagelser og skønsmæssige hensynsafvejninger, der gør det vanskeligt præcist at trække græn-

sen mellem det lovlige og det ulovlige. I eksemplet med e-mailudbyderen kan denne muligvis påberåbe sig, at brugeren af e-mailtjenesten via aftaleforholdet har givet samtykke til behandlingen, eller påberåbe sig undtagelsen om, at behandlingen (gennemsyn af e-mails med henblik på at identificere børnepornografisk materiale) er "nødvendig til varetagelse af en berettiget interesse og denne interesse klart overstiger hensynet til den registrerede". Hertil kommer, at det i forhold til digitale tjenester, der udbydes fra lande uden for EU, kan være vanskeligt at afgøre, om forholdet overhovedet omfattes af dansk eller EU's persondatalovgivning.

Det i dette afsnit anvendte eksempel har rod i en konkret sag, der har været omtalt i medierne, men skal for så vidt primært blot illustrere problemstillingens kompleksitet, herunder ikke mindst de mange regler og vanskelige afvejninger, der må inddrages og vurderes ved løsning af selv sager, der på overfladen virker enkle og forholdsvis ligetil.

10. Konklusioner og perspektivering

Det foregående har præsenteret en række forskellige områder og reguleringer, der har det til fælles at man på den ene side vil beskytte borgernes privatliv og på den anden side må have en række undtagelser og modifikationer til denne beskyttelse. I sagens natur har vi ikke lavet dybtgående juridiske analyser af disse enkeltområder, men har indskrænket os til at give et overblik over retsområdet og opridse og diskutere nogle hovedaspekter for at belyse, om der derigennem kan fremhæves nogle fælles træk og udfordringer.

Som det er fremgået, er grænsedragningsproblemer og brydninger mellem beskyttelse af privatlivets fred og beskyttelsen af andre samfundsvigtige interesser såsom bekæmpelse af kriminalitet og terror, indkrævning af den rigtige skat, bankers overholdelse af spillereglerne på de finansielle markeder osv., evig og uhyre vanskelig at arbejde med såvel generelt som konkret.

De grundlæggende rettigheder om privatlivets fred anerkender, at der konkret kan være andre interesser, det er vigtigere at varetage end fx retten til at kommunikere uden overvågning. For at denne legitime undtagelse imidlertid ikke skal kunne udnyttes til en intetsigende og reelt alt omfattende carte blanche til myndighederne, opstiller praksis efter EMD og EU-domstolen krav om, at undtagelserne skal præciseres i national lovgivning, ligesom det skal konkretiseres, hvorledes staterne undgår at udvande proportionalitetsprincippet fx i forbindelse med indsamling af data.

Efter praksis fra såvel EMD og EU-domstolen tegner der sig et mønster, hvorefter testen af, om de mange undtagelser er tilladelige i forhold til beskyttelsen af privatlivets fred, kan deles ind i følgende faser:

- Indsamlingen af data
  - Hvad er formålet med indsamlingen?
  - Hvor indgribende er midlet sammenholdt med formålet?
  - Hvor målrettet er indsamlingen - masseovervågning eller individuel overvågning?
  - Er der en uafhængig instans, der skal beslutte eller godkende indsamlingen, eller er det op til den indsamlende myndighed at afgøre?
- Anvendelsen af de indsamlede data
  - Er det muligt fra de indsamlede data kun at "udtrække" de helt nødvendige data?
  - Hvorledes håndteres de henholdsvis nødvendige og ikke-nødvendige data?
  - Må dataene videregives til andre myndigheder mv.?
  - Hvorledes sikres dataene mod udefrakommende angreb?
- Hvorledes forholdes der vedrørende overvågningens ophør?
  - Er der regler om sletning?
  - Er der regler om forudgående, samtidig eller efterfølgende underretning?

En række af de nævnte elementer indgår allerede i den gældende nationale lovgivning, men med meget forskellig tyngde og fokus. Den tydeligste - og største - beskyttelse ydes af reglerne i retsplejelovens kapitel 71, hvor der er konkret regulering af - og grænser for - samtlige faser.

Der er et særligt behov for at gennemarbejde disse problemstillinger i forhold til, hvilke hensyn er legitime hensyn til at gennembryde de grundlæggende rettigheder, hvor konkrete angivelser undtagelsesbestemmelserne skal indeholde, og hvorledes dette spiller sammen med en udbredt tendens hos lovgiver til samtidig at tillade specialmyndigheder at trænge ind på andres grund og indhente oplysninger alt uden

en retskendelse.[83] Et oplagt - og nyt - juridisk forskningsfelt vil således være at gennemanalysere de eksisterende regelsæt (hvoraf vi blot har nævnt de helt centrale) for at sammenholde dem med den ovenstående matrix.

Denne grundlæggende problemstilling lader sig imidlertid ikke se uden at inddrage mindst to yderligere perspektiver, der begge har udspring i det forhold, at internettet er globalt og at oplysninger og data vedrørende fysiske og juridiske personer ikke befinder sig et "sted i skyen", men relativt håndgribeligt enten på en server på et geografisk territorium eller er "undervejs" hen over/under andre territorier.

Det gælder for det første spørgsmålet om, hvorledes data er beskyttet på det sted, hvor de befinder sig, og dernæst spørgsmålet om, hvorvidt det har nogen betydning for den retlige vurdering heraf, at man ikke fysisk behøver at tage en tur f.eks. til Irland for at "åbne" serveren og tage dataene ud, men kan nøjes med at logge sig ind og helt ubesværet og friktionsløst hente de pågældende data fra København eller New York.

Disse tværnationale problemstillinger, som det ligger uden for rammerne for nærværende artikel at belyse, gør sig gældende ikke blot indenfor straffe- og straffeprocesretten, men i mindst lig så høj grad i forhold til alle speciallovgivningens kontrolregler. Samme globale grundvilkår gør sig gældende i forhold til politiets anvendelse af de tvangsindgreb, der er hjemlet i retsplejelovens kapitel 71. Kapitlet indeholder ingen regulering heraf, men Højesteret fastslog i en afgørelse fra 2012,[84] at dansk politi i forbindelse med en efterforskning af en dansk straffesag måtte "ransage" den sigtedes Facebook-profil, hvortil politiet havde adgangskoden, uagtet den server, hvor profilen blev opbevaret, befandt sig i Californien, og den sigtede i øvrigt havde anvendt profilen fra Canada. Højesterets begrundelse var alene, at det kunne lade sig gøre uden at involvere andre landes myndigheder.[85] Spørgsmålet er imidlertid om dette er den generelt "rigtige" tilgang, og hvis svaret herpå er bekræftende, må det overvejes om internettet herefter udgør en selvstændig jurisdiktion. Dette vil til gengæld medføre et utal af andre problemstillinger, så også her kaldes der på målrettet forskning.

Det samme gør anvendelsen af persondatalovgivningens mange undtagelser og hensynsafvejninger, ikke blot i forhold til offentlige myndigheders overvågning, men også den overvågning, ikke mindst i cyberspace, der i stigende grad udøves af private virksomheder. I den forbindelse er der også problemstillinger, retlige såvel som retspolitiske, knyttet til den overvågning, navnlig digitale overvågning, som private foretager på vegne af staten, fordi realiteten ofte er, at de data, som staten ønsker adgang til, genereres af private virksomheder og derfor mest enkelt og effektivt kan indsamles og - om nødvendigt - videregives af den private virksomhed. Det forhold, at staten på denne måde anvender private virksomheder i overvågningssammenhæng, aktualiserer i høj grad den ovenfor anførte "test" eller "matrix".

Noter

1. Også FN-systemet er optaget af de spørgsmål, vi behandler i denne artikel. Se fx FN-resolution 68/167, *The right to privacy in the digital age*. Vi har dog her valgt at fokusere på retskilder, der er direkte anvendelige i forholdet mellem myndigheder og borgere.

2. For relevant juridisk litteratur om emnet se fx *Birgitte Kofod Olsen & Rikke Frank Jørgensen* (red.), Overvågning eller omsorg - privatlivets grænser, Forlaget Thomson 2005, *Peter Blume & Janne Rothmar Herrmann*, Ret, privatliv og Teknologi, Jurist- og Økonomforbundets Forlag 2013, og følgende artikler i Juristen af *Peter Blume*: Overvågning (nr. 6, 2007, s. 183 ff.), Rettens begrænsede muligheder i forhold til overvågning (nr. 6, 2013, s. 251 ff.), Tv-overvågning (nr. 4, 2001, s. 144 ff.) og Offentliggørelse af tv-overvågning (nr. 4, 2008, s. 101 ff.). Af international litteratur kan nævnes FRA/CoE, Handbook on European data protection law (2014), med yderligere henvisninger s. 181 ff.

3. Jf. lovbekendtgørelse nr. 1190/2007

4. Jf. *Blume*, Rettens begrænsede muligheder i forhold til overvågning, Juristen nr. 6, 2013, s. 251 ff.

5. Som det fremgår af det følgende, vil masseovervågning udover en eventuel krænkelse af borgernes kollektive fred også kunne indebære en i hvert fald indirekte krænkelse af den enkeltes fred, uagtet dette ikke i første omgang er formå-

let med denne form for overvågning. Se hertil fx *Martin Scheinins* indlæg vedrørende NSAs masseovervågning under en høring i EU-parlamentet d. 14/10 2013 (kan læses på EU-Parlamentets hjemmeside).

6. I samme retning se fhv. folketingsdirektør og PET-chef *Ole Stig Andersens* indlæg ved det 38. Nordiske Juristmøde i København 2008.

7. Jf. EMRK-kommentaren s. 649 med henvisning til fx *S and Marper vs. UK*, dom af 4/12 2008, hvor det i pr. 66 udtales, at begrebet privatliv "is a broad term not susceptible to exhaustive definition. It covers the physical and psychological integrity of a person".

8. Jf. lovbekendtgørelse nr. 1190/2007.

9. Jf. fx *Niemitz*, dom af 16/12 1992 og *Bensaid*, dom af 6/2 2001.

10. Se om begrebet nærmere *Lorenzen* m.fl., Den Europæiske Menneskerettighedskonvention med kommentarer (herefter EMRK-kommentaren), Jurist- og Økonomforbundets Forlag 2011, s. 649 ff. og *Kjølbro*, Den Europæiske Menneskerettighedskonvention - for praktikere, Jurist- og Økonomforbundets Forlag 2010, s. 605 ff.

11. Af 7. december 2000. Charteret fik med Lissabon-traktaten traktatstatus.

12. Jf. *Neergaard & Nielsen*, EU-ret, Karnov Group 2010, s. 212.

13. Direktiv 95/46/EF og direktiv 2002/58/EF (som ændret ved direktiv 136/2009/EF).

14. Direktiv 2007/64/EF.

15. Se nærmere *Christensen m.fl.*, Dansk Statsret, Jurist- og Økonomforbundets Forlag 2012, s. 294.

16. Se nærmere *Sandfeld Jakobsen & Schaumburg-Müller*, Medieretten, Jurist- og Økonomforbundets Forlag 2013, s. 208.

17. Jf. straffelovens § 263, stk. 1, nr. 3

18. Jf. straffelovens § 264a, modsætningsvist.

19. Jf. lov nr. 429/2000 med senere ændringer.

20. I den i medfør af teleloven udstedte udbudsbekendtgørelse, jf. bkg. nr. 715/2011. Se om bekendtgørelsen nærmere *Sandfeld Jakobsen* (red.), Teleretten, Jurist- og Økonomforbundets Forlag 2014, s. 162 ff.

21. Se også *Blume & Herrmann*, Ret, privatliv og teknologi, Jurist- og Økonomforbundets Forlag 2013, s. 42.

22. Jf. nærmere *Korfits Nielsen & Waaben*, Lov om behandling af personoplysninger med kommentarer, Jurist- og Økonomforbundets Forlag 2008, ad § 1, stk. 2.

23. Jf. nærmere *Blume* i UfR 2002B.456 ff.

24. Se nærmere *Sandfeld Jakobsen* (red.), Teleretten, Jurist- og Økonomforbundets Forlag 2014, s. 151 ff.

25. Se nærmere sundhedslovens kap. 9.

26. Jf. lov om finansiel virksomhed kap. 9.

27. Jf. nærmere *Sandfeld Jakobsen & Schaumburg-Müller*, Medieretten, Jurist- og Økonomforbundets Forlag 2013, s. 157 f.

28. Det følger af det almindelige forvaltningsretlige legalitetsprincip, at forvaltningsmyndigheder skal have hjemmel til de aktiviteter, de udfører.

29. Jf. EMRK-kommentaren s. 766.

30. Jf. fx Blecic mod Kroatien, dom af 29.07.04 og uddybende *Kjølbro*, Den Europæiske Menneskerettighedskonvention - for praktikere, Jurist- og Økonomforbundets Forlag 2010, s. 599 ff.

31. Jf. *Kjølbro*, Den Europæiske Menneskerettighedskonvention - for praktikere, Jurist- og Økonomforbundets Forlag 2010, s. 600 ff.

32. Jf. straffelovens § 1, hvorefter straf kun kan pålægges for et forhold, hvis strafbarhed er hjemlet

ved lov, eller som ganske må sidestilles med et sådant.

33. Se herom nærmere *Langsted & Waaben*, Strafferettens almindelige del I, Karnov Group 2011, s. 65 og 96 ff., samt *Baumbach*, Det strafferetlige legalitetsprincip, Jurist- og Økonomforbundets Forlag 2008, især s. 453 ff.

34. Jf. betænkning 601/1971, s. 58.

35. Se for norsk rets tilsvarende problem vedrørende leddet "uberettiget" i relation til hacking mv.: *Inger Marie Sunde*, Lov og rett i cyberspace, Fagbokforlaget, Bergen 2006, s. 144 ff.

36. Se nærmere *Sandfeld Jakobsen & Schaumburg-Müller*, Medieretten, Jurist- og Økonomforbundets Forlag 2013, s. 176 ff.

37. Datatilsynet har gennem sin praksis naturligvis gradvist bidraget til at klargøre og præcisere reglerne, men tilsynets praksis vedrørende overvågning koncentrerer sig primært om tv-overvågning. Se om fortolkning af persondatalovens undtagelsesregler i forhold til tv-overvågning *Blume*, Tv-overvågning, Juristen nr. 4, 2001, s. 144 ff.

38. Der er ikke helt enighed i teorien om, hvornår man kan karakterisere et efterforskningsskridt som et "tvangsindgreb", se nærmere diskussion og henvisninger i *Toftegaard Nielsen*, Straffesagens Gang, 5. udg., Jurist- og Økonomforbundets Forlag 2011, s. 82 ff., og *Smith* m.fl. Straffeprocessen, 2. udg., Forlaget Thomson 2008, s. 417 ff. Bredest tilslutning har dog fortsat *Gammeltoft-Hansens* definition, jf. Straffeprocessuelle tvangsindgreb, Juristforbundets Forlag, 1981, s. 44 f., hvorefter et tvangsindgreb groft sagt er skridt, som det ville være strafbart for en almindelig borger at foretage. Derfor skaber reglerne i retsplejeloven hjemmel for politiet til at foretage sådanne skridt, ligesom reglerne regulerer, hvornår og hvordan politiet kan foretage de enkelte efterforskningsskridt.

39. Jf. retsplejelovens § 788.

40. Nærmere reguleret i retsplejelovens § 791.

41. Jf. retsplejelovens § 789.

42. Hermed forstås jf. retsplejelovens § 791a, stk. 2: "fjernbetjent eller automatisk virkende tv-kamera, fotografiapparat eller lignende apparat eller ved hjælp af et apparat, der anvendes i boligen". Hverken betænkningen (Bet. 1298/1995) eller lovforslaget (lovforslag nr. 41 af 8. oktober 1998) uddyber, hvad der tænkes på med ordene "… et apparat, der anvendes i boligen…", men såvel en formåls- som en ordlydsfortolkning må føre til, at dette også omfatter programmer, der kan aktivere et web-kamera med tilhørende mikrofon, der befinder sig i rummet, hvorved udefra kommende vil kunne høre samtaler og optage billeder af, hvad der foregår.

43. Jf. retsplejelovens §§ 780 ff.

44. Ved afgørelsen af om det er tilladeligt at opsætte tv-overvågning skal de almindelige forvaltningsretlige regler være opfyldt. se f.eks. *Blume* i UfR 2010B.36 ff. Lov om tv-overvågning regulerer stort set udelukkende privates tv-overvågning.

45. Bekendtgørelsen (nr. 988) er fra 28/9 2006, men blev ændret ved bekendtgørelse nr. 660 af 19/6 2014, således at der ikke længere er krav om sessionslogning det vil sige hvilke IP-numre, der har været i kontakt med hvilke andre IP-numre (altså en tilsigtet registrering af hvilke internetsider hver enkelt bruger havde været inde på). Der er dog fortsat krav om logning af telefoni-kommunikation. Det skal endvidere fortsat registreres, når et IP nummer kobles på internettet samt placeringen af denne opkobling, hvis den sker trådløst, jf. logningsbekendtgørelsens § 5, stk. 1.

46. Logningsbekendtgørelsens § 4

47. I de forenede sager *C-239/12 og C-594/12*.

48. 2006/24/EF af 15 marts 2006.

49. http://justitsministeriet.dk/sites/default/files/media/Pressemeddelelser/pdf/2014/Notat%20om%20logningsdirektivet.pdf

50. I en note til notatets konklusion henvises til en forudgående forklaring om, at man fra ministeriets side ville ophæve kravet om sessionslogning.

Ikke fordi det angiveligt var i strid med EU-reglerne, men fordi "erfaringerne [har] vist, at oplysningerne kun i meget begrænset omfang er brugbare i praksis i forbindelse med efterforskning og retsforfølgning af strafbare forhold." Man kunne på den baggrund dog godt overveje, om kravet om proportionalitet mellem indgrebet og dens betydning i bekæmpelsen af grov kriminalitet har været opfyldt. Herom er notatet imidlertid tavst.

51. Se præmis 56-59.

52. I præmis 56.

53. Se kritisk overfor Justitsministeriets notat og lovligheden af logningsbekendtgørelsen endvidere Jacob Mchangama i tænketanken Justitia's notat af 4. september 2014, jf. (http://justitia-int.org/wp-content/uploads/2014/09/Analyse_Revision-af-logningsreglerne_sep142.pdf)

54. Jf. PET-lovens § 5

55. Jf. PET-lovens § 4

56. Om reguleringen af PET og dettes funktioner se i det hele *Greve*, Politiets efterretningstjeneste, Jurist- og Økonomforbundets Forlag 2014.

57. Jf. PET-lovens § 10 og FE-lovens § 7.

58. Jf. lov. Nr. 602 af 12/6 2013, § 3.

59. Jf. FE-lovens § 6

60. Jf. FE-lovens § 7, stk. 2, jf. § 4

61. Lov nr. 713 af 25/6 2014 om Center for Cybersikkerhed.

62. Bl.a. § 4.

63. Jf. § 9, stk. 1

64. Jf. PET-lovens kapitel 9 samt lov om Center for Cybersikkerhed, § 19

65. Jf. fx *Rotaru*, dom af 4/5 2000, og *Segerstedt-Wiberg m.fl.*, dom af 6/6 2000.

66. Jf. *S og Marper mod UK,* dom af 4/12 2008.

67. Ibid.

68. Jf. fx *Malone*, dom af 2/8 1984, *Amann*, dom af 16/2 2000, og *Liberty m.fl.*, dom af 1/7 2008.

69. Jf. EMRK-kommentaren s. 765-66 med relevante domshenvisninger.

70. Jf. navnlig *S and Marper mod Storbritannien*, dom af 4/12 2008, og *M.K mod Frankrig*, dom af 18/4 2013.

71. Se nærmere *Blume og Rothmar Herrmann*, Ret, privatliv og teknologi, s. 292 ff.

72. Jf. e-datadirektivets art. 5 og 15.

73. Se nærmere *Sandfeld Jakobsen* (red.), Teleretten, Jurist- og Økonomforbundets Forlag 2014, s. 154 f.

74. Jf. præmis 61.

75. Sml. EMD's afgørelse i *Amann*, dom af 16/2 2000, og afsnit 6.1 ovenfor.

76. Jf. telelovens § 10 og nærmere i *Sandfeld Jakobsen* (red.), Teleretten, Jurist- og Økonomforbundets Forlag 2014, s. 181 ff.

77. Jf. luftfartslovens § 148 a.

78. Jf. lov om forebyggende foranstaltninger mod hvidvask af udbytte og finansiering af terrorisme kap. 3.

79. Ifølge retspraksis fra EMD har staten således positive forpligtelser i tilfælde, hvor der er en direkte og umiddelbar forbindelse mellem de ønskede foranstaltninger og vedkommendes privatliv og/eller familieliv, jf. *Kjølbro*, Den Europæiske Menneskerettighedskonvention - for praktikere, Jurist- og Økonomforbundets Forlag 2010, s. 624 f.

80. Om charterets direkte virkning se nærmere *Neergaard & Nielsen*, EU-ret, Karnov Group 2010, s. 221 f.

81. Det kan så diskuteres, hvor langt private - her e-mailudbyderen - skal gå for at bekæmpe kriminalitet, idet dette jo som udgangspunkt er en opgave, som varetages af politi og anklagemyndighed.

82. C-275/06, jf. nærmere *Sandfeld Jakobsen* i Juristen nr. 10, 2008, s. 305 ff.

83. Direkte begrundet af Justitsministeriet i forbindelse med en sådan hjemmel i revisorloven med, at der jo alligevel ikke var noget for en dommer at tage stilling til, hvis hjemmelen er tilstrækkeligt åben. Se nærmere *Langsted* i "En fit and proper lov?", i antologien Retssikkerhed i Konkurrence med andre hensyn (Carsten Munk-Hansen (red)), Jurist- og Økonomforbundets Forlag 2012, s. 191.

84. Offentliggjort i Ugeskrift for Retsvæsen 2012.2614 H

85. Afgørelsen er kommenteret af *Langsted* i Digital Evidence and Electronic Signature Law Review, nr, 10, 2013, s 164 f.