KAPITEL 9

Medier og persondata

Opdatering pr. oktober 2020 ved forfatterne
Søren Sandfeld Jakobsen og Sten Schaumburg-Müller

1. Indledning og disposition

Oplysninger om personer indgår som et helt væsentligt led i mediers virke i form af både neutrale oplysninger, billeder og vurderinger. Persondataretten[1] omfatter som udgangspunkt al automatisk behandling af personoplysninger, og selvom journalistisk virksomhed i vidt omfang er undtaget, er det oplagt at se nærmere på, hvilken rolle denne lov spiller på det medieretlige område.

Tidligere var persondataretten reguleret via den danske persondatalov, der igen byggede på et EU-direktiv.[2] Fra 25 maj 2018 består reguleringen imidlertid både af en EU-forordning, der gælder direkte i Danmark, og af en lov, vedtaget af det danske Folketing. Der er således hele tiden to regelsæt, man skal have sig for øje, henholdsvis persondataforordningen[3] (GDPR) og databeskyt-

1. Termen bruges om den samlede regulering, dvs. både EU-regulering og dansk national regulering. Efter 2018 bruges ofte betegnelsen »databeskyttelse« på området, men eftersom der er tale om beskyttelse af persondata, benytter vi fortsat termen persondataret.
2. Persondataloven (PDL), lov 429/2000 med en del senere ændringer, og Direktiv 95/46/EF 24.10.1995 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger.
3. Med den samlede titel: Europa-Parlamentets og Rådets Forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (generel forordning om databeskyttelse). Forkortelsen GDPR er taget fra den engelske tekst General Data Protection Regulation.

telseslov (DBL).[4] Desuden gælder lov om massemediers informationsdatabaser (MDL),[5] der særskilt regulerer mediers databaser.

Persondataretten er et tværgående felt, der som udgangspunkt gælder, så snart der sker en automatisk behandling af persondata. Området er reguleret på den specielle måde, at hvis en behandling er omfattet, hvilket meget ofte vil være tilfældet, så skal der findes en bestemmelse, der giver mulighed for denne behandling. Eller sagt på en anden måde: Hvis ikke det eksplicit er tilladt, er det forbudt – det modsatte af, hvad vi kender fra fx straffeloven.

Med persondataloven fra år 2000 blev det tidligere Registertilsyn ændret til Datatilsynet, der bl.a. fører tilsyn med området, træffer afgørelser, meddeler påbud og forbud mv. Praksis fra Datatilsynet er således relevant for forståelsen af gældende ret. Her skal man være opmærksom på, at tidligere afgørelser ikke nødvendigvis vil være relevante efter den ny ordnings gennemførelse. Ofte vil dette dog være tilfældet, eftersom de nye danske regler efter databeskyttelsesloven på mange områder ligger meget tæt op af de hidtidigt gældende regler.[6]

Også domme fra EU-Domstolen er relevante. EU-Domstolen kan træffe bindende afgørelser om fortolkning af forordningen,[7] – men selvfølgelig ikke om den danske lovgivning. Som eksempel kan nævnes sagen Satamedia Oy C-73/07, omtalt nærmere nedenfor afsnit 2.3, der bestemmer, at »journalistisk virksomhed« skal forstås bredt og ikke kan indskrænkes til traditionelle journalistiske mediers aktiviteter. Sagen blev afgjort efter det tidligere direktiv, men er fortsat relevant, da forordningen har overtaget opfattelsen af, at journalistik skal forstås bredt, jf. præamblens pkt. 153.[8] Domme afsagt efter det tidligere direktiv kan således være relevante, men forordningen har på en del områder lagt op til en ny retstilstand, og på de områder er de tidligere afgørelser selvfølgelig mindre relevante. Der vil formentlig gå et par år, inden EU-Domstolen tager stilling til sager efter den nugældende forordning.

4. Lov 502/2018 med den samlede titel: Lov om supplerende bestemmelser til forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (databeskyttelsesloven).
5. Lov 430/1994.
6. Datatilsynet har på sin hjemmeside lagt praksis efter den tidligere regulering under »Historiske afgørelser«: https://www.datatilsynet.dk/tilsyn-og-afgoerelser/historiske-afgoerelser/ tilgået 12. oktober 2020.
7. Dette sker typisk ved de såkaldte præjudicielle afgørelser: En national domstol kan forelægge et spørgsmål, der vedrører EU-retten, for EU-Domstolen. Dette er et praktisk system, der er med til at sikre en ensartet gennemførelse af EU-retten i de mange medlemslande, men selvfølgelig ikke noget, der bidrager til hurtig sagsbehandling.
8. Forordningen består ligesom andre EU-regler af et sæt bindende regler, formuleret i artikler, svarende til de danske §§. Forinden er der en »præambel«, en fortale, der principielt ikke er en bindende tekst, men dog må inddrages i forståelsen af reglerne.

I det følgende behandles persondatarettens dækningsområde, altså spørgsmålet om, hvilke former for behandling af personoplysninger, der er omfattet, i afsnit 2. I afsnit 3 redegøres kort for de relevante hovedtræk, der gælder, når en persondatabehandling er omfattet. Disse regler er komplicerede, og for en nærmere analyse henvises til den eksisterende speciallitteratur. For nærværende omtales kun i hovedtræk, hvilke regler der skal opfyldes, hvis en form for medievirksomhed skulle blive omfattet. I afsnit 4 behandles spørgsmålet om personbilleder – også en form for persondatabehandling – og i afsnit 5 redegøres der nærmere for databaser, herunder naturligvis især mediers databaser, reguleret ved særlig lov. Endelig i afsnit 6 behandles tv-overvågning, der også anses for behandling af persondata, jf. DBL § 2, stk. 4.

2. Behandling af personoplysninger – udgangspunkt, undtagelser og undtagelsesundtagelser

2.1. Udgangspunkt

Persondatarettens anvendelsesområde er uhyre bredt.

En personoplysning forstås som »enhver form for information om en identificeret eller identificerbar fysisk person«, GDPR art. 3, nr. 1. Der skal være tale om en fysisk person, altså et menneske, ikke et dyr, ikke en fiktiv person og ikke en juridisk person (et firma, et ApS etc.). En fysisk person kan dog hurtigt komme ind i billedet: Hunden har en ejer, den fiktive person har en forfatter, og er et firma i enmandseje, vil omtalen af firmaet typisk også omfatte personen. I Danmark gælder beskyttelsen indtil 10 år efter vedkommendes død, DBL § 2, stk. 5, og under graviditet må moren være den beskyttede.

For at være omfattet af regelsættet, skal den pågældende være identificerbar. En effektiv anonymisering bringer forholdet uden for persondataretten.

Også »oplysning« skal forstås bredt: Et billede af en person er en personoplysning, selvom det i daglig sprogbrug virker kunstigt at tale om et billede som en oplysning. Også meningstilkendegivelser om identificerbare personer er omfattet, »X er en idiot« (hvor X er en identificerbar person), og det samme gælder urigtige oplysninger, »X er 175 cm høj«, selvom X faktisk er en del højere. Alt sammen er oplysninger i persondatarettens forstand.

Som udgangspunkt er al »automatisk behandling« af personoplysninger omfattet, jf. GDPR art. 2, stk. 1, og DBL § 1, stk. 2, og også »behandling af personoplysninger (…) der er eller vil blive indeholdt i et register« er omfattet, selvom behandlingen ikke er automatisk. Ikke-automatisk behandling er fx, når mennesker taler sammen personligt. Her vil der jævnligt blive udvekslet personoplysninger, men persondataretten gælder ikke, allerede fordi behandlingen

ikke er automatisk. Andre love kan være relevante, fx STL § 264 d om uberettiget videregivelse af private meddelelser eller billeder.[9]

Behandling defineres som »enhver aktivitet eller række af aktiviteter – med eller uden brug af automatisk behandling – som personoplysninger eller en samling af personoplysninger gøres til genstand for ...«, art. 3, nr. 2, og der nævnes som eksempler: »[I]ndsamling, registrering, organisering, systematisering, opbevaring, tilpasning eller ændring, genfinding, søgning, brug, videregivelse ved transmission, formidling eller enhver anden form for overladelse, sammenstilling eller samkøring, begrænsning, sletning eller tilintetgørelse.« Ikke bare registrering, men stort set al behandling af oplysninger om identificerbare personer er således i udgangspunktet omfattet af loven.

Fra dette omfattende udgangspunkt er der imidlertid en række undtagelser:

2.2. Undtagelse. Hensyn til informations- og ytringsfriheden

Ifølge DBL § 3, stk. 1, finder hverken loven eller forordningen anvendelse, hvis det vil være i strid med informations- og ytringsfriheden, jf. EMRK art. 10.[10] Bestemmelsen synes på én gang selvfølgelig og ejendommelig: For det *første* gælder EMRK art. 10 under alle omstændigheder som en del af dansk ret,[11] og den bliver ikke mere gældende af også at være nævnt her. For det *andet* er det vel ikke særlig oplagt at sige, at hele databeskyttelsesloven og forordningen slet ikke gælder i tilfælde af sammenstød med ytrings- og informationsfriheden. Snarere er det mere oplagt at erindre om, at dette hensyn skal inddrages i fortolkningen. Dette synes også at være Datatilsynets forståelse, jf. nedenfor.[12] Og for det *tredje* gælder ikke kun EMRK art. 10 om ytrings- og informationsfrihed, men også art. 8 om beskyttelse af privatlivet, der ofte kan trække i en anden retning end ytrings- og informationsfriheden. At nævne EMRK art. 10 kunne således nok være på sin plads, men uden at nævne de til tider modstående hensyn i art. 8 kan dette give anledning til en skævhed i vægtningen og i værste fald forkerte afgørelser.[13]

9. Se herom nærmere *Medieretten* 2020, kap. 4, afsnit 4, og *Mediejura for journalister og andre mediearbejdere* 2016, kap. 3, afsnit 4.
10. Se også Sandfeld Jakobsen & Schaumburg-Müller, »Persondatabehandling i journalistisk øjemed«, *Juristen* 2017, s. 53-62.
11. Jf. inkorporeringsloven, lbkg. 750/1998.
12. Se nærmere Blume i UfR 2003B.215f.: »Databeskyttelse og ytringsfrihed«.
13. I Satamedia Oy, C-73/07, der vedrører offentliggørelse af privatpersoners skatteoplysninger, herunder via en sms-tjeneste, understreger EU-Domstolen eksplicit behovet for en »afbalanceret afvejning« af de to grundrettigheder. Informations- og ytringsfriheden har således ikke forrang for beskyttelsen af privatlivet.

Hensynet til ytringsfriheden har spillet en afgørende rolle i flere afgørelser fra Datatilsynet: En afgørelse fra 2000[14] drejede sig om Dansk Folkepartis offentliggørelse af navne og bopælskommuner på 3.218 personer, der havde fået indfødsret, sammen med oplysninger om, at flere af personerne havde straffedomme eller gæld til det offentlige. Datatilsynet lagde vægt på, *at* navnene i forvejen var offentligt tilgængelige, *at* der var tale om en politisk tilkendegivelse, og *at* oplysningerne om kriminalitet mv. ikke refererede til bestemte personer, og afgørelsen fremstår på den baggrund som velbegrundet. Tilsyneladende mente Datatilsynet, at oplysningerne om kriminalitet og gæld var »meningstilkendegivelser«, hvilket virker mindre overbevisende: Oplysning om kriminalitet og gæld er faktiske oplysninger, men mindre problematiske, når de ikke knyttes til enkeltpersoner og indgår i en debat af offentlig interesse.

I en afgørelse fra 2006,[15] havde et firma på sin hjemmeside kritisk kommenteret et besøg fra Arbejdstilsynet med angivelse af navn, stilling, uddannelse og arbejdssted på den pågældende medarbejder. Også her lægger Datatilsynet vægt på, at der er tale om meningstilkendegivelser og subjektive vurderinger. Det er oplagt, at et firma eller andre må kunne kritisere en offentlig myndighed, men dette indebærer ikke nødvendigvis, at en enkelt medarbejder uden videre kan nævnes og identificeres. I sin praksis efter de tidligere gældende regler har Datatilsynet vægtet ytringsfriheden på bekostning af beskyttelse af privatliv i situationer, hvor hensynet til ytringsfriheden udmærket kunne være varetaget uden at genere den enkelte medarbejder ved offentliggørelse af navn mv. Datatilsynet har med vedtagelsen af nye regler nu en mulighed for at ændre praksis.

Datatilsynet fulgte samme linje i en afgørelse vedrørende Det Sorte Register.[16] Her registreres oplysninger fra borgere, der har følt sig uretfærdigt behandlet. Hjemmesiden understreger, at de registrerede ikke nødvendigvis har begået noget forkert eller ulovligt, men registreringen sker under overskrifter som »pligtforsømmelser«, »magtmisbrug« mv. Oplysninger vedrører ofte en person i et firma eller en offentlig institution, og personen angives typisk med navn, stillingsbetegnelse, arbejdstelefon, til tider med fødselsdato, politisk tilhørsforhold, selskabets CVR-nummer mv. Datatilsynet afviste at foretage sig noget og henviste til, »at hjemmesidens tema er forholdet mellem borgere og beslutningstagere/myndighedspersoner, at hjemmesiden er præget af subjek-

14. DT j.nr. 2000-236-0005.
15. DT j.nr. 2006-215-0309 af 2. oktober2006.
16. DT j.nr. 2011-215-0874 af 12. juni2012.

tive vurderinger og værdiladede ytringer, og at de påklagede oplysninger indgår som en del af meningstilkendegivelserne«. Datatilsynet synes at mene, at når personoplysninger blot behandles som led i en subjektiv meningstilkendegivelse, falder de uden for persondataloven. Dette er næppe rigtigt, hverken i forhold til EU-retten eller til den europæiske menneskeret.[17]

Efter vores vurdering bør Datatilsynet benytte lejligheden til bedre at afbalancere praksis. Selvfølgelig skal der tages hensyn til ytrings- og informationsfriheden, men dette bør ikke ske på bekostning af beskyttelsen af privatlivet i bred forstand. Både EMD og danske domstole er udmærket i stand til både at beskytte ytringsfriheds- og informationsfriheden og samtidig tage hensyn til beskyttelse af de involverede mere private interesser.[18]

2.3. Undtagelse. Personlig eller familiemæssig aktivitet

Efter GDPR art. 2, stk. 2, litra c, gælder forordningen ikke for behandlinger »som foretages af en fysisk person som led i rent personlige eller familiemæssige aktiviteter«. Undtagelsen gælder således kun fysiske personer, ikke virksomheder eller foreninger. Firmaer, skoler, menighedsråd, foreninger o.lign. vil således alle skulle opfylde persondatarettens krav.

For at være undtaget skal behandlingen desuden være rent personlig eller familiemæssig. Hvad dette nærmere betyder, er ikke ganske klart. På den ene side må fx upubliceret slægtsforskning, fotos til familiealbum, adressefortegnelser på egen mobiltelefon, private presseklip mv. falde uden for forordningen. På den anden side er alle kommercielle eller erhvervsmæssige aktiviteter ikke »personlige« i forordningens forstand og falder derfor under forordningens mange regler, også selvom aktiviteten foretages af en fysisk person. En person, der overvejer at starte egen it-virksomhed, vil således være omfattet af persondataretten fx ved indsamling af oplysninger om potentielle kunder, også selvom de første kunder skulle være at finde i familie- eller vennekredsen, mens den samme persons adressefortegnelse af samme familie og venner ikke vil være omfattet.

17. Og heller ikke efter dansk strafferet. Retten i Holbæk har ved dom af 6. januar 2014 fundet en del af oplysningerne på hjemmesiden strafbare efter STL § 267, pålagt at de fjernes og tillagt de omtalte en godtgørelse for tort.
18. Se fra dansk ret fx U 2012.1788H, hvor Højesteret anså en udsendelse om forholdene på et plejehjem for værende af almen interesse, altså beskyttelse af informations- og ytringsfriheden, men samtidig understregede at visning af en beboers »vask forneden« på ingen måde var nødvendig for at opnå formålet. Spørgsmålet er nærmere behandlet *Medieretten* kap. 4 og *Mediejura for journalister og andre mediearbejdere* kap. 3. EMD har tilsvarende fx i Gourgénidze (Gurgenidze) v Georgien 17. oktober 2006 statueret krænkelse af art. 8 i forbindelse med offentliggørelse af et personfoto i en sag, der i øvrigt havde offentlig interesse.

I præamblens pkt. 18 hedder det: »[K]orrespondance og føring af en adressefortegnelse eller sociale netværksaktiviteter og onlineaktiviteter, der udøves som led i sådanne aktiviteter«, og der er hermed lagt op til en udvidelse af privat-undtagelsen. Formuleringen må indebære, at i hvert fald en del aktiviteter, herunder på nettet, falder uden for persondatarettens strenge regimente. Fotografering til privat brug, også af personer i det offentlige rum, og upload af billeder på Instagram el.lign. af familie, venner eller folk på gaden må derfor kunne være uden for persondatarettens rækkevidde. (Se også om personbilleder nedenfor afsnit 4). Hvor langt undtagelsen strækker sig efter de nye regler er endnu ikke klart, men der må være et område, der nok ikke er kommercielt, men alligevel heller ikke kan siges at være en rent personlig eller familiemæssig aktivitet. Som eksempel kan nævnes den såkaldte »Viborg-mappe«, hvor billeder af unge kvinder deles, helst så mange, så nøgne og så eksplicitte som muligt. Selvom aktiviteten ikke er kommerciel – der foregår muligvis en betaling, men der byttes også bare – kan den næppe siges at være »rent personlig eller familiemæssig.« Det samme må gælde fx politikeres Facebook-sider og Twitter-konti: Her henvender kendte personer sig til offentligheden, og de personoplysninger, der måtte forekomme, må være reguleret af persondataretten. I hvilket omfang dette også gælder for mere ukendte personers kommunikation henstår pt. uafklaret. Her må der lægges vægt på, hvor personlig og familiemæssig kommunikationen er. En Facebook-profil, der nok i princippet er lukket, men som i realiteten omfatter mange hundrede »venner«, kan efter vores vurdering ikke opfattes som »rent personlig«.

Man skal her være opmærksom på, at undtagelsen fra persondatarettens regler ikke gælder for den dataansvarlige eller for databehandlere, der »tilvejebringer midlerne« for persondatabehandlingen.[19] Dette betyder, at aktører som Facebook og Instagram fortsat skal overholde persondatarettens regler, også når den private aktør er undtaget efter art. 2, stk. 2, litra c.[20]

19. Præamblens pkt. 18, sidste sætning.
20. Spørgsmålet om, i hvilket omfang medier som fx Facebook kan blive strafferetligt ansvarlige for indhold, som andre har lagt op, er behandlet i Schaumburg-Müller, »Strafansvar for indholdet af onlinemedier - Om formidleransvar for medier, der ikke er omfattet af medieansvarsloven«, U 2018B.113-123.

Enhver persondatabehandling, der foretages af en juridisk person som fx et firma, en organisation eller en forening, er omfattet af persondataretten.
Enhver kommerciel persondatabehandling er omfattet af persondataloven.
Rent personlig eller familiemæssig perondatabehandling er ikke omfattet, og det gælder også aktiviteter på nettet.
Hvor langt denne undtagelse rækker er pt. ikke ganske afklaret.

Det skal understreges, at andre regler fortsat gælder, herunder fx straffelovens regler om fotografering af personer på ikke frit tilgængeligt sted, § 264 a, og videregivelse af private oplysninger og meddelelser, § 264 d. Her skal man være opmærksom på, at reglerne ikke er sammenfaldende.[21] Fx vil det være strafbart efter STL § 264 a at fotografere ind i naboens have, hvor der er børnefødselsdag, mens fotograferingen vil være undtaget persondataretten, hvis fotograferingen kun er til personligt eller familiemæssigt brug.

2.4. Undtagelser for medier mv.

Efter GDPR art. 85, stk. 1, »forener [medlemsstaterne] ved lov retten til beskyttelse af personoplysninger i henhold til denne forordning med retten til ytrings- og informationsfrihed, herunder behandling i journalistisk øjemed og med henblik på akademisk, kunstnerisk eller litterær virksomhed«. De forskellige hensyn skal altså »forenes«, og art. 85, stk. 2, forudsætter, at dette gøres ved, at medlemsstaterne fastsætter undtagelser og fravigelser for hvert enkelt kapitel i persondataforordningen (dog undtaget kapitlet med sanktioner). I databeskyttelsesloven er der dog ikke foretaget detaljerede overvejelser, og »foreningen« er blot sket ved en bloc-undtagelser i fem bestemmelser, § 3, stk. 4-8, der igen kan inddeles i tre grupper: databaser, stk. 4-6, manuelle udklip, stk. 7, og behandling i journalistisk øjemed i øvrigt, stk. 8, første led. Den danske løsning er ikke i overbevisende overensstemmelse med forordningen.[22]

Efter DBL § 3, stk. 4, er databaser, der er omfattet af lov om massemediers informationsdatabaser, (MDL), ikke omfattet af persondataretten. Ideen er, at det skal være muligt for massemedier at have databaser med personoplysninger uden at skulle opfylde de til tider strenge – og for massemedier i realiteten umulige – krav til persondatabehandling. Loven er behandlet nedenfor afsnit 2.5.

21. *Medieretten,* kap. 4, og *Mediejura for journalister og andre mediearbejdere*, kap. 3.
22. Se nærmere Søren Sandfeld Jakobsen og Sten Schaumburg-Müller, »Persondatabehandling i journalistisk øjemed«, *Juristen*, 2017, s. 54-62.

Efter § 3, stk. 7, finder »loven ... ikke anvendelse på manuelle arkiver over udklip fra offentliggjorte, trykte artikler, som udelukkende behandles i journalistisk øjemed. Dog gælder bestemmelserne i GDPR art. 28 og 32 (om disse se nedenfor afsnit 2.6 og 2.7). Det kan være svært at se et særligt område for stk. 7, der blot synes at være et specialtilfælde af »behandlinger ... i journalistisk øjemed«, der er undtaget efter stk. 8.

Efter stk. 8 er persondatabehandling »som i øvrigt udelukkende finder sted i journalistisk øjemed« også undtaget fra lovens bestemmelser (ligeledes undtagen GDPR art. 28 og 32, der således også gælder for journalistisk virksomhed).

Bestemmelsen i stk. 8 er ligesom stk. 7 uafhængig af tilknytning til et medieansvarslovsmedie, og det må herefter tages stilling om aktiviteten »udelukkende finder sted i journalistisk øjemed«.

Her er det klart, at mediers abonnementskartoteker o.lign. ikke har noget med den særlige undtagelse at gøre. Når det drejer som om sådanne aktiviteter, skal medier overholde persondataretten som alle andre.

I artikel 85 står der ikke nærmere om, hvad der skal forstås ved »journalistisk øjemed«, men det fremgår af betragtning 153, at begrebet »journalistisk« ikke må fortolkes snævert af hensyn til den betydning, som de journalistiske medier har for et demokratisk samfund. Det vil sige, at medlemsstaterne ikke må fastsætte undtagelser for behandling med et journalistisk øjemed, der kun er forbeholdt de egentlige og etablerede nyhedsmedier, man sædvanligvis forbinder med journalistik. Begrebet er bredere og skal kunne omfatte alle, der persondatabehandler i journalistisk øjemed. »Journalistisk øjemed« er således ikke et organisatorisk begreb, hvor der ses på tilknytningen til etablerede medier, men et funktionelt begreb: Kan den pågældende aktivitet med rimelighed siges at være journalistisk?[23] Det er på den ene side klart, at det ikke er tilstrækkeligt, at den pågældende påberåber sig at være journalist.[24] Der må være realitet i påstanden. På den anden side kan man ikke kræve tilknytning til et etableret medie, men også bloggere o.a. kan falde under undtagelsen.

Er der ikke tale om en aktivitet, der på nogen meningsfuld måde kan betegnes som »journalistisk øjemed«, kan aktiviteten dog stadig være undtaget fra persondataretten ud fra hensynet til informations- og ytringsfriheden, jf. afsnit 2.1 ovenfor.

Hertil kommer kravet om, at aktiviteten »udelukkende« er i journalistisk øjemed for at kunne falde under undtagelsen.[25] Dette må betyde, at aktiviteter, der også i nogen grad er private, ikke kan blive omfattet af undtagelsen. Mange

23. Se også Satamedia Oy C-73/07, pr. 61.
24. Se Bet. 1565/2017, »Databeskyttelsesforordningen – og de retlige rammer for dansk lovgivning«, Del 1, bd. 2, bd. s. 951.
25. Jf. præambel nr. 153.

billeder, videoer og tekster, der lægges på f.eks. Facebook, vil formentlig være en sådan blanding af privat og lettere journalistisk karakter. Man fortæller på én gang om, hvad man selv oplever, *og* om noget, der kan have en vis offentlig interesse. Efter forordningen vil sådanne oplægninger ikke være omfattet af den journalistiske undtagelse, da der ikke er tale om en aktivitet, der *udelukkende* er journalistisk.[26]

I sådanne tilfælde kan andre undtagelser være relevante: Der kan være tale om rent personlige og familiemæssige aktiviteter, jf. GDPR art. 2, stk. 2, litra c (nærmere omtalt kapitel 4, afsnit 3), og der kan være tale om information, der falder under den generelle beskyttelse af ytrings- og informationsfriheden, jf. for dansk rets vedkommende DBL § 3, stk. 1 (nærmere omtalt i kapitel 7).

2.5. Undtagelser for kunstnerisk eller litterær virksomhed

Efter § 3, stk. 8, 2. pkt., er »behandling af oplysninger, som udelukkende sker med henblik på kunstnerisk eller litterær virksomhed« også undtaget fra persondataretten, men på samme måde som journalistisk virksomhed efter 1. pkt. således at GDPR art. 28 og 32 finder anvendelse, jf. nedenfor afsnit 2.6 og 2.7. »Litterær virksomhed« kan anvendes i tilknytning til journalistisk øjemed, fx ved behandling af persondata i forbindelse med research til bog. Også fagbøger er omfattet af litterær virksomhed, jf. DT 26.3.2004, mens behandling af personoplysninger i forbindelse med forskning ifølge Waaben og Nielsen ikke vil kunne omfattes af denne bestemmelse.[27] Persondataforordningen indeholder dog andre regler om brug af persondata i forskningen, og GDPR art. 85 pålægger medlemsstaterne også at beskytte akademisk virksomhed ud over den kunstneriske og litterære. Dette er dog ikke medtaget i de danske regler, hvor DBL § 3, stk. 8, kun undtager kunstnerisk og litterær virksomhed. Spørgsmålet forfølges ikke yderligere her.

2.6. Andre undtagelser

Der er andre undtagelser fx for anklagemyndighed og Folketinget. Dette behandles ikke nærmere her, og der henvises til speciallitteraturen.

26. Se dommen Sergejs Buivids C-345/17, nærmere omtalt i Bent Ole Gram Morten (red.), *Dansk Persondataret*, ExTuto, kap. 22.
27. Waaben og Nielsen (2015), s. 125.

Persondataretten regulerer behandling af persondata. Alle oplysninger om og billeder af personer er persondata.

Personlig og familiemæssig behandling er undtaget. Upload på (i realiteten) åbne internetsider og tv-overvågning ud over ens egen grund falder *ikke* under denne undtagelse.

Medier er undtaget – på tre forskellige måder:

– Medier, der er omfattet af medieansvarsloven (MAL), kan have deres egne databaser uden at skulle opfylde persondatalovens mange og komplicerede krav. Til gengæld skal mediedatabaselovens betingelser være opfyldt.
– Manuelle, journalistiske arkiver er næsten helt undtaget. Elektroniske arkiver er *ikke* omfattet af denne undtagelse, der således kun har en begrænset anvendelse
– Al journalistisk virksomhed i øvrigt – dvs. ud over pkt. 1 og 2 – er næsten helt undtaget fra persondataretten. Denne undtagelse forudsætter *ikke* tilknytning til medieansvarsloven.

2.7. Undtagelsesundtagelse. Regler der også gælder for databehandling i journalistisk øjemed: Art. 28

Som nævnt ovenfor er behandling af personoplysninger i »journalistisk øjemed« ikke omfattet af loven, DBL § 3, stk. 8, dog således at art. 28 og 32 alligevel gælder.

Artikel 28 indeholder særlige regler om forholdet mellem den dataansvarlige og databehandleren. Overordnet betyder det, at hvis man sender databehandling ud af huset, herunder til en »cloud«-løsning, skal art. 28 overholdes. Og med DBL § 3, stk. 8, gælder dette også for databehandling i journalistisk øjemed.

Persondataretten skelner mellem to relevante aktører: den dataansvarlige og databehandleren. Ifølge art. 4, nr. 7, er den dataansvarlige den, »der alene eller sammen med andre afgør, til hvilke formål og med hvilke hjælpemidler der må foretages behandling af personoplysninger«, mens en databehandler er den, »der behandler personoplysninger på den dataansvarliges vegne«, jf. art. 4, nr. 8. Sondringen mellem databehandleren og den dataansvarlige er juridisk vigtig og i princippet simpel, men i praksis ikke altid så let. De engelske udtryk kan måske hjælpe: Den dataansvarlige er »controller«, og behandleren er »processor«. Inden for medieverdenen betyder dette, at medievirksomheden er dataansvarlig, og medarbejderne på mediet arbejder for den dataansvarlige og hører ind under dennes ansvar. Medarbejderne, herunder de journalistiske, er altså

ikke databehandlere i persondatarettens forstand, selvom de i en vis dagligdags forstand netop behandler en masse personoplysninger. Medarbejderne udgør en enhed med virksomheden, der er dataansvarlig. Først hvis noget af databehandlingen sendes ud af huset, fx fordi mediet ikke selv vil håndtere de mere praktiske aspekter, er den, der sørger for fx opbevaring af data at betragte som databehandler. Her erindres om, at også opbevaring udgør en behandling i persondatarettens forstand, art. 4, nr. 2. Er man ansat som journalist el.lign. på en medievirksomhed, behøver man således ikke bekymre sig om art. 28.

Arbejder man derimod freelance, forstås situationen bedst således, at man som freelancer er dataansvarlig, og her må man selv sørge for at overholde art. 28's mange forskrifter. Når det her formuleres lidt forsigtigt, skyldes det, at der ikke i forbindelse med tilblivelsen af databeskyttelsesloven er taget stilling til, hvorledes art. 28 passer til medieverdenen. Men det rigtigste må være, at den journalist (fotograf mv.), der arbejder selvstændigt også selvstændigt har forpligtelser efter art. 28. Persondatabehandling i journalistisk virksomhed kan siges at have det privilegium at være undtaget fra persondatarettens mange regler, hvorfor det forekommer rimeligt at stille krav til især sikkerheden af behandlingen.

Art. 28 stiller i korte træk krav om følgende:

- For at kunne bruge en databehandler, skal denne stille fornødne garantier for at kunne opfylde kravene efter forordningen, for journalistisk virksomheds vedkommende kravene efter art. 32.
- Databehandleren må ikke uden aftale videregive behandlingen til andre. Her må gælde, at hvis databehandler er en virksomhed, kan databehandling organiseres *inden for* virksomheden, men ikke ud af huset til tredjepart.
- Forholdet mellem den dataansvarlige (fx freelance-journalisten) og databehandleren skal være reguleret af en kontrakt eller et EU-retligt dokument (se herom nedenfor), og kontrakten skal bl.a. indeholde bestemmelser om, *at* databehandleren kun må behandle efter instruks fra den dataansvarlige, *at* ansatte hos databehandler er undergivet tavshedspligt, *at* art. 32 skal overholdes, *at* databehandleren skal bistå den dataansvarlige med at overholde de relevante regler (her igen for journalistisk virksomhed art. 32), og som udgangspunkt *at* data slettes, når kontrakten mellem de to parter ophører. Desuden skal databehandleren kontraktmæssigt forpligtes til at give den dataansvarlige mulighed for at påse, at behandlingen foregår retmæssigt.

Art. 28, stk. 5-8, muliggør, at man kan benytte på forhånd godkendte standardkontrakter. Det er her forudsat, at både EU-Kommissionen og tilsynsmyndigheden, dvs. Datatilsynet, kan fastsatte standardkontraktbestemmelser. Der ses

i skrivende stund, juli 2018, ikke at være udfærdiget særlige standardbestemmelser med henblik på journalistisk virksomhed, og det er næppe heller sandsynligt, at det vil ske.

2.8. Undtagelsesundtagelse. Regler der også gælder for databehandling i journalistisk øjemed: Art. 32

Art. 32 relaterer sig til datasikkerhed, hvilket selvfølgelig også er relevant for medier. Efter bestemmelsens stk. 1, litra a-d, er der fire områder, hvor man især skal være opmærksom og aktiv.

For det *første* skal man overveje pseudonymisering og kryptering af personoplysninger, litra a). Journalister ligger jævnligt inde med følsomme oplysninger. Pseudonymisering, dvs. man omdøber personer til koder, der ikke umiddelbart er genkendelige,[28] er formentlig mindre praktisk i det daglige journalistiske arbejde, hvor det normalt vil være vigtigt at kunne identificere netop den person, man skal tale med eller tale om. Man bør derfor overveje kryptering, især hvis man har at gøre med meget følsomme oplysninger.

For det *andet* skal man overveje »evne til at sikre vedvarende fortrolighed, integritet, tilgængelighed og robusthed af behandlingssystemer og -tjenester«, som det hedder i litra b). Ideen er, at man skal gennemtænke de forskellige situationer, man er i, forsøge at identificere risiciene og så imødegå disse. Efter sigende har russiske journalister aldrig deres mobil tændt i metroen eller andre steder, hvor der er mange mennesker, fordi de mener sig udsat for noget, der ligner andet og mere end almindeligt tyveri. Samme risiko er der næppe i Danmark, men det er relevant at overveje risikoen for tyveri og risikoen for, at andre uberettiget kan få adgang til fx hemmelige kilder eller andre beskyttelsesværdige personoplysninger.

Det *tredje* punkt er juridisk set mindre relevant for journalister, nemlig evnen »til rettidigt at genoprette tilgængeligheden af og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk hændelse«, jf. litra c. Journalister m.fl. har netop ikke en forpligtelse til fx at orientere de registrerede (»datasubjekterne«), ændre dataene på anmodning og slette efter brug (se nedenfor afsnit 3 om de almindelige regler i persondataretten). Men journalister har selvfølgelig selv en interesse i, at oplysninger om kilder og kontakter ikke pludselig forsvinder eller bliver hacket.

Endelig som det *fjerde* punkt kræver litra d) »en procedure for regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske foranstaltninger til sikring af behandlingssikkerhed.« Ideen er, at det ikke er nok, at man har tænkt sikkerhed, da man installerede sin software eller

28. Forordningen definerer nærmere i art. 4, nr. 5.

fik sin mobil mv. Den skal løbende evalueres, både hackere og venligtsindede it-firmaer bliver konstant mere sofistikerede og dygtige, så hvad der var effektivt for et år siden, er det ikke nødvendigvis længere. Desuden bør man også tjekke egne procedurer: Husker man at slukke eller i hvert fald lukke for skærmen, hvis man forlader mobilen osv., og ved man fortsat, hvad man skal gøre, hvis man bliver udsat for ondsindede angreb, enten fysisk eller virtuelt.

Listen er principielt ikke udtømmende,[29] men det er et godt sted at starte.

Hvad man mere præcist skal gøre, afhænger af en række faktorer. I art. 32, stk. 1, hedder det:

> Under hensyntagen til det aktuelle tekniske niveau, implementeringsomkostningerne og den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder gennemfører den dataansvarlige og databehandleren passende tekniske og organisatoriske foranstaltninger for at sikre et sikkerhedsniveau, der passer til disse risici [...].

Og stk. 2 udtrykker sig på lignende måde:

> Ved vurderingen af, hvilket sikkerhedsniveau der er passende, tages der navnlig hensyn til de risici, som behandling udgør, navnlig ved hændelig eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger, der er transmitteret, opbevaret eller på anden måde behandlet.

Ideen må være, at sikkerhedsforanstaltningerne gennemtænkes, vurderes, implementeres, gennemprøves og dokumenteres. Som det kan ses af formuleringerne, indgår en meget lang række hensyn, fx både omkostninger og risici. Man behøver således ikke nødvendigvis gøre alt, hvad der er muligt, men blot alt hvad der er rimeligt. De mange forskelligartede vægte i vægtskålen gør afvejningsresultatet temmelig uforudsigeligt, men der er næppe tvivl om, at en veloovervejet sikkerhedspolitik lettere vil blive accepteret, også selvom der sker brud, mens en ikke-gennemtænkt, ikke-dokumenteret og/eller ikke-efterprøvet lettere vil kunne ende i sanktioner, herunder bøde (omtalt nedenfor afsnit 2.8)

Forholdet til mediedatabaselovens sikkerhedskrav til interne, dvs. redaktionelle databaser (omtalt nedenfor afsnit 5.2), er ikke uden videre klart. Det må dog være således, at de krævede »fornødne sikkerhedsforanstaltninger«, jf. MDL § 5, nu skal forstås i lyset af art. 32's noget mere udspecificerede og omfattende krav.

29. Jf. formuleringen i art. 32, umiddelbart før de fire punkter: »herunder bl.a.«.

2.9. Undtagelsesundtagelse. Regler der også gælder for databehandling i journalistisk øjemed: GDPR kapitel VIII

Det følger af både GDPR art. 85 og DBL § 3, stk. 5-8, at journalistisk virksomhed – her helt på linje med litterær, kunstnerisk og akademisk virksomhed – *ikke* er undtaget fra GDPR kapitel VIII. Kapitlet har overskriften »Retsmidler, ansvar og sanktioner«, og i det følgende ses på de regler, der kan være relevante for journalistisk virksomhed.

Efter art. 77 har enhver ret til at klage til en relevant tilsynsmyndighed, jf. også DBL § 39. Dette indebærer formentlig, at Datatilsynet fremover skal behandle klager over journalister m.fl., hvis klagen vedrører art. 28 eller 32. Hvis man fx er kilde hos en journalist, vil man til Datatilsynet kunne klage over manglende sikkerhed efter art. 32 og manglende overholdelse af reglerne for brug af databehandler efter art. 28.[30]

Art. 78 kræver effektive retsmidler i forhold til tilsynsmyndighederne, hvilket i Danmark vil sige Datatilsynet. Dette krav må i almindelighed siges at være opfyldt. Der er efter de almindelige regler mulighed for at indbringe myndigheder for domstolene, hvilket endog er skrevet ind i Grundlovens § 64.

Art. 79 kræver effektive retsmidler over for både dataansvarlige og databehandlere. Dette er i princippet også opfyldt, men måske ikke i politiets og anklagemyndighedens praksis.

Art. 82 sætter regler for erstatning, der næppe bringer særligt nyt i forhold til de almindelige danske erstatningsregler. Der henvises til speciallitteraturen.

Art. 83 bestemmer bl.a., at der i visse tilfælde kan gives bøder op til € 10 mio. eller 2 % af virksomhedens samlede omsætning, hvis dette er højere, og i andre tilfælde op til € 20 mio. eller 4 % af omsætningen. Der er lagt op til et markant anderledes bødeniveau end det gængse i Danmark, og hvad medieretten angår, er det værd at notere sig, at journalistisk virksomhed ikke er undtaget. Især hændelige brud på sikkerheden, jf. art. 32, kan tænkes at være relevant: Journalister, fotografer og andre, der i øvrigt er omfattet af undtagelsen til persondataretten, herunder freelancere, risikerer betragtelige bøder, hvis sikkerheden ikke er i orden.

30. Problemet er her, at DBL § 3, stk. 4, bestemmer, at loven og databeskyttelsesforordningen slet ikke finder anvendelse på behandlinger, der er omfattet af lov om massemediers informationsdatabaser«, mens GDPR netop ikke giver nogen mulighed for undtagelser efter forordningens kap. VIII.

3. Nogle hovedregler i persondataretten

Som det fremgår af ovenstående, vil en medievirksomhed normalt ikke være underlagt databeskyttelseslovens regelsæt (med undtagelse af GDPR art. 28 og 32).

Der kan dog forekomme situationer, hvor lovens omfattende regelsæt skal iagttages, således fx hvis en mediedatabase ikke opfylder betingelserne efter DBL § 3, stk. 4-6, eller hvor en aktivitet, der involverer behandling af persondata, nok har et publikum, men ikke kan siges at være hverken journalistisk, litterær, kunstnerisk eller akademisk.

3.1. Grundlæggende principper

Art. 5 indeholder »Principper for behandling af personoplysninger«: Al behandling skal således ske »lovligt, rimeligt og på en gennemsigtig måde«, jf. art. 5, stk. 1, litra a. Kravet om lovlighed indebærer, at enhver behandling, der falder inden for forordningen, skal have lovhjemmel. Hvis man behandler persondata, fx tager et billede med en person på eller skriver noget om en person, skal man kunne finde en bestemmelse i forordningen (eller loven), der gør, at en sådan behandling er lovlig, medmindre behandlingen falder helt uden for, som fx privatbehandling og behandling i »journalistisk øjemed«, jf. ovenfor afsnit 2. Selvom kravet til lovlighed er opfyldt, er dette ikke tilstrækkeligt. Behandlingen skal også være rimelig, hvilket bl.a. indebærer, at man ikke må behandle overflødige mængder data, jf. umiddelbart nedenfor.

Endelig er der princippet om gennemsigtighed, der stiller krav til den dataansvarlige og databehandleren: Der skal være klarhed over, hvorledes oplysningerne behandles, klarhed over sikkerhedsforanstaltninger mv.

Art. 5, stk. 1, litra b, kræver formålsbegrænsning, og personoplysninger skal »indsamles til udtrykkeligt angivne og legitime formål og må ikke viderebehandles på en måde, der er uforenelig med disse formål«. Efter tidligere lovgivning var der et krav om, at oplysninger kun måtte bruges til det oprindelige formål, men dette er nu blødt op, således at oplysningerne blot ikke må bruges på en måde, der er i modstrid med det oprindelige formål.

Litra c indeholder et krav om dataminimering: Man må ikke behandle ud over, hvad der er nødvendigt i forhold til formålet.

Som eksempel kan nævnes et forslag om gennemsyn af studerendes computere efter en skriftlig stedprøve.[31] Forslaget lever ikke op til kravet om dataminimering. Det er på den ene side helt legitimt at kontrollere for snyd ved eksamen, men et gennemsyn af *hele* indholdet af en anvendt computer er skudt langt over målet. Etablering af et overvågningssystem, der tjekker fx skærm og eksterne forbindelser *under* eksamen synes derimod acceptabelt – selvfølgelig under den forudsætning, at der ikke overvåges andet, og at overvågningen reelt stopper ved eksamenens afslutning.

Art. 5, litra d, kræver »rigtighed«, at man skal sørge for, at behandlede data er korrekte, og urigtige oplysninger skal derfor enten slettes eller korrigeres. Oplysninger må heller ikke opbevares i længere tid end nødvendigt, jf. art. 5, stk. 1, litra f, og endelig skal oplysninger behandles på en sikker måde, således at personoplysninger ikke (let) lækkes eller hackes.

Det er i sidste ende den dataansvarlige, der har ansvaret for disse grundlæggende regler holdes, jf. art. 5, stk. 2.

Art. 4 indeholder den persondataretlige definition af en lang række termer, og her er især samtykke relevant. Samtykke kan meget ofte være afgørende i forhold til, om behandling er lovlig, men det skal understreges, at samtykke aldrig er eneste kriterium. Art. 4, nr. 11, definerer samtykke som »enhver frivillig, specifik, informeret og utvetydig viljestilkendegivelse«. Frivillighed er vel overraskende, men der ligger heri, at samtykke skal være en reel valgmulighed, og ved vurdering skal der tages hensyn til parternes styrkeforhold.[32] Specifikation indebærer, at det nærmere må fremgå, hvad samtykket angår: Er det fx kun indsamling til særlig brug, fx videnskabelig, eller er det videreudnyttelse også i kommerciel sammenhæng. Og kravet om information understreger, at den samtykkende skal vide, hvad der samtykkes til. Dette skal således fremgå klart, også når der er tale om standardvilkår, jf. også præamblens nr. 39 og især 42. Endelig indeholder betingelsen »utvetydig«, at samtykket er kommet til udtryk enten sprogligt eller ved klart bekræftende adfærd.[33] Stiltiende samtykke – altså det at man ud fra situationen forstår, at der er samtykke

31. Udkast fra Styrelsen for Undervisning og Kvalitet, dateret 19. september 2017, til Bekendtgørelse om visse regler om prøver og eksamen i de gymnasiale uddannelser, § 6, stk. 6.
32. Jf. præamblen pkt. 32 og 43. Se for en detaljeret gennemgang af samtykke Working Paper (WP) 259 af 28. november 2017, udarbejdet af den daværende Art. 29-gruppe og efterfølgende godkendt af det nu oprettede Databeskyttelsesråd.
33. WP 259, pkt. 3.4.

– kan være tilstrækkeligt på strafferettens område,[34] men ikke på persondatarettens.

Art. 7 og 8 indeholder yderligere regler om samtykke. Det er den dataansvarlige, der skal kunne dokumentere, at der foreligger samtykke, art. 7, stk. 1, et samtykke kan altid tilbagekaldes, stk. 3, og ved vurdering af, om et samtykke faktisk er givet frit, skal der tages hensyn til, om samtykket i sin udstrækning har været nødvendigt, stk. 4. Samtykke kan gives af børn fra 13 år, jf. GDPR art. 8 og DBL § 6.

Endvidere skal man være opmærksom på, at kravet ved de særligt følsomme oplysninger (se herom umiddelbart nedenfor) er yderligere skærpet: Her kræves tillige, at samtykket er »udtrykkeligt«, GDPR art. 9, stk. 2, litra a, hvilket indebærer krav om skriftlighed eller ved elektronisk kommunikation en totrinsaccept, hvor man efter at have accepteret får en email eller sms, som så skal bekræftes.[35]

3.2. Krav til behandling og kategorier af personoplysninger

Et helt centralt element i persondataretten er kravet om lovgrundlag. Hvis en aktivitet er inden for persondatarettens brede område, og hvis aktiviteten ikke er undtaget, skal man have lov til at foretage den pågældende behandling. Sagt lidt mere teknisk: Behandlingen skal have hjemmel i en lovbestemmelse. Man skal altså ind i persondatarettens regler for at se, om man kan finde en bestemmelse, der giver mulighed for at foretage den behandling, man har tænkt sig at foretage.

I DBL § 6, stk. 1, hedder det: »Behandling af personoplysninger må finde sted, hvis mindst en af betingelserne i databeskyttelsesforordningens artikel 6, stk. 1, litra a-f, er opfyldt.« De vigtigste af disse behandles nedenfor, afsnit 3.2.1. Hvis der er tale om en »følsom personoplysning« gælder en række yderligere forbud, jf. DBL § 7 og GDPR art. 9,[36] nedenfor afsnit 3.2.2. »Oplysninger om strafbare forhold« har sin egen danske regel i DBL § 8, afsnit. 3.2.3. Hertil kommer en række andre kategorier som fx retsinformationssystemer, §

34. Se *Medieretten* kap. 4, afsnit 2.4.1 og *Mediejura for journalister og andre mediearbejdere* kap. 3, afsnit 2.5.
35. WP 257, pkt. 4, s. 18.
36. Tidligere ansås art. 9, stk. 2, for selvstændigt behandlingsrundlag, således at man skulle finde et behandlingsgrundlag *enten* for de følsomme oplysninger *eller* for de almindelig Pr. 7. november 2019 har Datatilsynet imidlertid annonceret, art. 9 ikke udgør et behandlingsgrundlag, men alene et forbud med undtagelser. Opfattelsen er nærmere begrundet i Datatilsynets baggrundsnotat af samme dato.

9, statistiske eller videnskabelige undersøgelser, § 10, personnumre, § 11 m.fl. Disse sidste kategorier behandles ikke for nærværende.

3.2.1. Personoplysninger generelt

De grundlæggende krav til behandling af personoplysninger er reguleret i GDPR art. 6.

For det *første* kan der ske lovlig behandling, hvis den pågældende har givet samtykke, jf. art. 6, stk. 1, litra a. Bemærk, at der inden for persondataretten gælder særlig krav til samtykke, jf. ovenfor afsnit 3.1.

For det *andet* kan der ske behandling, hvis det er nødvendigt til opfyldelse af en kontrakt, jf. art. 6, stk. 1, litra b. Der et vist overlap med samtykke – en kontrakt uden nogen form for samtykke er ikke en kontrakt – men kontrakten en gensidig, hvilket typisk indebærer, at den ene part ikke blot kan opsige. Dette er i modsætning til et samtykke, der i persondataretten typisk altid kan tilbagekaldes. Ved arbejdskontrakter er det nødvendigt at behandle personoplysninger, men bestemmelsen giver kun mulighed for at behandle de *nødvendige* oplysninger.

Hertil kommer en række muligheder i art. 6, stk. 1, litra c, d og e, som ikke behandles nærmere her.

I litra f finder vi den vigtige afvejningsregel: Hvis den dataansvarlige har en legitim og tungerevejende interesse end den registrerede, kan der ske behandling. Dette betyder, at den dataansvarlige – som både kan være den person, der uploader personoplysninger på sin åbne Facebookprofil, og den store virksomhed, der behandler oplysninger om sine mange ansatte – må gøre sig overvejelser over, netop om behandlingsinteressen vejer tungere end beskyttelsesinteressen.

Hvis den registrerede selv har offentliggjort oplysningen (herunder billedet), vil dette tale for lovligheden af yderligere behandling.[37] »Selvoffentliggørelse« er ikke særskilt reguleret i art. 6, men må vurderes efter afvejningsreglen. Ofte vil selvoffentliggørelse medføre, at videre behandling er lovlig efter art. 6, stk. 1, litra f, men det gælder ikke al viderebehandling som anvendelse i krænkende sammenhæng (fx billeder, der manipuleres ind i en pornografisk sammenhæng) eller brug i reklame el.lign.

37. Bemærk, at der typisk også vil være ophavsret involveret, og her gælder ingen selvoffentliggørelsesregel.

Kravet om afvejning vil også indebære, at den, der faktisk har overvejet pro et contra vil stå stærkere end den, der blot behandler personoplysninger uden nærmere overvejelser.[38]

Offentlige myndigheder kan ikke bruge afvejningsreglen, men må finde en anden bestemmelse for lovligt at kunne behandle personoplysning.

3.2.2. Følsomme oplysninger

Til de følsomme oplysninger hører »[O]plysninger om race eller etnisk oprindelse, politisk, religiøs eller filosofisk overbevisning eller fagforeningsmæssigt tilhørsforhold samt behandling af genetiske data, biometriske data med det formål entydigt at identificere en fysisk person, helbredsoplysninger eller oplysninger om en fysisk persons seksuelle forhold eller seksuelle orientering«. Sådanne oplysninger er undergivet et strammere regimente, idet GDPR art. 9 indeholder egentlig forbud mod behandling undtagen i nærmere definerede tilfælde.

Oplysninger om sygdom er omfattet af de strammere regler, og det samme gælder oplysninger om politisk overbevisning og fagforeningsmæssige tilhørsforhold.

Art. 9 sætter en længere række specificerede undtagelser fra forbuddet, hvoraf her kun to kort skal omtales:

Samtykke er – selvfølgelig – også relevant, hvad de følsomme oplysninger angår. Samtykke forstås som »enhver frivillig, specifik, informeret og utvetydig viljestilkendegivelse«, jf. art. 4, nr. 11, omtalt ovenfor afsnit 3.1. Hertil kommer for de følsomme oplysningers vedkommende, at samtykket skal være »udtrykkeligt«. Hvad dette yderligere krav nærmere betyder, er ikke ganske klart. I forarbejderne angives det, at kravet til udtrykkelighed ikke giver nogen særlig forskel ud over at skærpe opmærksomheden på samtykket, jf. betænkning 1565, s. 208. Efter nærværende forfatteres vurdering holder betragtningen ikke i detaljen. Der er forskel på et samtykke, der er udtrykkeligt (»explicit« som det hedder i den engelske udgave), og et stiltiende (eller underforstået) samtykke, også selvom de øvrige betingelser er opfyldt. Set fra databehandlerens side er det således tilrådeligt at gå videre end blot en åbenlys indforståethed, selvom denne klart måtte fremgå af situationen. Det bemærkes, at det under alle omstændigheder er databehandleren, der skal dokumentere et samtykke, jf. art. 7, stk. 1.

38. Se fx uploaderens bemærkning i U 2019.1415H (Moren og blotteren): »jeg vil skide højt og flot på hans følelser«, hvilket åbenlyst ikke udgør en indikation på afvejning af interesser. Det skal bemærkes, at Højesteret endte med at afvise sagen, fordi anklagemyndigheden havde forsøgt at køre sagen to gange.

Selvoffentliggørelse er selvstændig nævnt i art. 9, stk. 2, litra e: Behandling er ikke forbudt, hvis den »vedrører personoplysninger, som *tydeligvis* er offentliggjort af den registrerede« (forf.s kursivering). Den dataansvarlige skal sikre sig, at den følsomme oplysning, der kan foreligge i form af et billede, er offentliggjort af den pågældende, og ikke bare er offentligt tilgængelig. Oplysninger kan være offentliggjort på retsstridig vis, og selv lovlige oplysninger fx fra medier – der netop normalt ikke er omfattet af persondatarettens regler, jf. DBL § 3, stk. 4-8 – vil normalt kun kunne viderebehandles, hvis de er kommet frem på den omtaltes foranledning.

Der er ikke nævnt nogen afvejningsregel, når det drejer sig om følsomme oplysninger. Det betyder, at det ikke er muligt at behandle følsomme personoplysninger med henvisning hertil. Der skal findes en undtagelse fra forbuddet i art. 9, stk. 2, og herefter skal der findes et lovgrundlag i art. 6. Hvis en følsom oplysning er offentliggjort af den pågældende selv, fx på en åben Facebookprofil, er der ikke noget forbud efter art. 9, og herefter kan afvejningsreglen i art 6, stk. 1, litra f, anvendes. Der skal således også ved en selvoffentliggørelse fortsat foretages en afvejning.

Teknisk set er den detaljerede regulering svær at håndtere. Man skal både læse (og forstå) GDPR art. 9, den meget, men ikke fuldstændig tilsvarende regulering i DBL § 7, og art. 6, hvortil kommer muligheden for at sætte undtagelser efter en bekendtgørelse, altså uden om lovgivningsmagten, jf. DBL § 7, stk. 5. Dette forslag har været genstand for omfattende kritik.

For medieretten er det relevante de to nævnte undtagelser: samtykke og selvoffentliggørelse.

3.2.3. Strafbare forhold

GDPR art. 10 overlader det til medlemsstaterne at regulere behandling af oplysninger om strafbare forhold, dog på visse betingelser: Enten skal behandlingen foretages under kontrol af en offentlig myndighed, og ellers kan private foretage behandling, når det er indskrevet i lovgivningen og med »passende garantier for registreredes rettigheder og frihedsrettigheder«. Registre over straffedomme må kun føres under tilsyn af offentlig myndighed

DBL § 8 regulerer behandlingen af straffedomme for dansk rets vedkommende.

Termen »strafbare forhold« dækker bredt og omfatter både selve gerningen eller mistanke herom, den eventuelle straffesag, og efterfølgende oplysninger om afsoning og om den tidligere straffedom. Under »strafbare forhold« hører også rettighedsfrakendelse. Hvis en person er frakendt retten til at være advokat, er dette en oplysning om strafbart forhold i persondatarettens forstand.

Man kan overveje, om også forkerte oplysninger om strafbare forhold hører under bestemmelsen. Hvis en person udsættes for en chikanøs politianmeldelse, der intet har på sig, har den pågældende ikke begået noget strafbart (mens anmelderen eventuelt kan pådrage sig straf, jf. straffelovens § 165), og det kan derfor virke søgt at tale om strafbare forhold.[39] På den anden side er urigtige personoplysninger også omfattet af persondataretten – med ret til korrektion eller sletning, jf. GDPR art. 5 og 16 – og en urigtig oplysning om strafbare forhold synes derfor bedst at skulle behandles efter reglerne for denne type oplysninger: Der er ingen grund til, at en urigtig oplysning om strafbare forhold skulle behandles efter art. 6 med dennes mere omfattende hjemmelsgrundlag.

Den danske regulering i databeskyttelseslovens § 8 er bygget op på den måde, at offentlige myndigheders behandling reguleres i stk. 1 (behandling generelt) og stk. 2 (særligt om videregivelse), og privates behandling af oplysninger om personers strafbare forhold er reguleret i stk. 3 (behandling generelt) og stk. 4 (særskilt om videregivelse). Endelig bestemmer stk. 5, at oplysninger om personers strafbare forhold kan behandles, hvis betingelserne for behandling følsomme oplysninger er opfyldt. For nærværende behandles reguleringen for offentlige myndigheder ikke.

Man skal – selvfølgelig – være opmærksom på andre regler i persondataretten. Sker omtalen af strafbare forhold i personlig venne- eller familiekreds, falder situationen helt udenfor persondataretten, jf. GDPR art. 2, stk. 2, litra c, og sker behandlingen i journalistisk øjemed, gælder særlige regler (se ovenfor afsnit 2).

Efter Datatilsynets praksis bliver mere løse beskyldninger kategoriseret som »meningstilkendegivelser«, der helt er undtaget persondataretten efter DBL § 3, stk. 1, om ytrings- og informationsfrihed. Hvis beskyldningerne derimod er specificerede og velbegrundede, skal § 8 anvendes. Det giver den ejendommelige situation, at ubegrundede beskyldninger om strafbare forhold frit kan behandles, mens begrundede beskyldninger kun må behandles efter de strammere krav i databeskyttelseslovens § 8. Datatilsynets praksis er nok praktisk på den måde, at tilsynet slipper for at behandle sager om ubegrundede beskyldninger, men den er ikke i god overensstemmelse med ytrings- og informationsfriheden, hvor netop de velbegrundede og sande beskyldninger nyder en langt større beskyttelse end ubegrundede beskyldninger.[40]

39. Betænkning 1565, s. 233-234 afviser, at sådanne forkerte oplysninger kan falde under kategorien »strafbare forhold«.
40. Se f.eks. EMD Medzlis Islamske Zajednice Brcko v Bosnien-Herzegovina 7. juni 2017 GC, hvor en national dom med sanktioner for ærekrænkende udtalelser imod en navngiven person fandtes at være overensstemmende med ytrings- og informationsfriheden, fordi beskyldningerne ikke var velbegrundede.

Der er to muligheder for privates behandling af oplysninger om personers strafbare forhold, nemlig udtrykkeligt samtykke og en vægtet afvejning.

Hvad *samtykke* angår, skal dette være udtrykkeligt, ligesom ved behandling af følsomme oplysninger. Hertil skal samtykket opfylde de almindelige persondataretlige krav: Samtykket skal være frivilligt, specifik, informeret og utvetydigt.

Om den *vægtede afvejning* siger § 8, stk. 3: »behandling (kan) ske, hvis det er nødvendigt til varetagelse af en berettiget interesse og denne interesse klart overstiger hensynet til den registrerede.« Der stilles således skærpede krav til afvejningen i forhold til artikel 6, stk. 1, litra f. Dette giver god mening, da oplysninger om strafbare forhold kan være mere følsomme end almindelige oplysninger som navn og telefonnummer – uden dog at strafbare oplysninger behandles som en følsom oplysning efter GDPR art. 9.

Forarbejder lægger op til, at bestemmelsen kun undtagelsesvist kan anvendes. Det kunne f.eks. være registrering af strafbare forhold med henblik på at indgive politianmeldelse og eventuelt senere vidneforklaring i retten. Og af hensyn til den registrerede nævnes, at en organisation som Amnesty International må behandle oplysninger, f.eks. fordi den pågældende person ikke kan findes eller ikke kan kontaktes på grund af fængsling.[41]

Den tilsvarende formulering i stk. 4 er en smule anderledes, men forskellen til formuleringen i stk. 3 er blot, at det i stk. 4 er udspecificeret, at der både kan være tale om private og offentlige interesser, og at interessen kan ligge hos den registrerede. Dette vil også være tilfældet efter stk. 3.

Et tilsyneladende udbredt fænomen på internettet går ud på at omtale eller advare imod personer, der menes at have begået noget strafbart eller i hvert fald noget dadelværdigt eller irriterende.

Retsstillingen kan skitseres som følger:

Efter *straffeloven* kan det være strafbart at beskylde andre for noget kriminelt eller andet, der kan være alvorligt f.eks. i forhold til erhverv, job mv., jf. STL §§ 267-269. Ubegrundede beskyldninger og formodninger (om lidt grovere forhold) kan derfor være strafbare, og det samme gælder udbredelse og videregivelse af rygter (fortsat af grovere karakter), der ikke har nogen faktuel dækning, ud over at der er et rygte. (Se nærmere kap. 4 i *Mediejura for journalister og andre mediearbejdere* eller andre fremstillinger).

Efter *persondataretten* ser det noget anderledes ud. Hvis der ikke er samtykke – og det vil der i praksis sjældent være – så kan oplysninger om strafbare forhold kun undtagelsesvist behandles. Interessen i behandlingen, her i form af omtale på nettet, skal veje markant tungere end den registreredes interesse i

41. Betænkning 1565, s. 238-239.

ikke at få sine (mulige) strafbare forhold offentlig omtalt. Og det vil sjældent være tilfældet. Heller ikke i tilfælde, hvor den pågældende tages på fersk gerning f.eks. via tv-overvågning, må det strafbare forhold videregives til offentligheden, men gerne til politiet.[42] Som ovenfor nævnt vil mere løse beskyldninger blive kategoriseret som meningstilkendegivelser, hvorfor de efter Datatilsynets praksis ikke er omfattet af persondataretten. Hertil skal man være opmærksom på, at beskyldninger mod firmaer kun er omfattet af persondataretten, hvis beskyldningen er rettet mod en fysisk person. Virksomheder er ikke beskyttet efter *person*dataretten.

3.3. Den registreredes rettigheder

GDPR kapitel III omhandler den registreredes rettigheder: Den registrerede skal som udgangspunkt have visse basale *oplysninger* om behandlingen, art. 13 og 14, den registrerede har en *indsigtsret*, således at der skal gives nærmere oplysninger efter anmodning, art. 15, en ret til *berigtigelse*, art 16, og en ret til *sletning* efter art. 17. Denne sidste ret benævnes også »retten til at blive glemt«, hvilket er misvisende.[43] Der er en ret til under visse betingelser at blive slettet hos den pågældende dataansvarlige, fx hvis oplysningerne behandles ulovligt, art. 17, stk. 1, litra d, eller hvis samtykket kaldes tilbage, og der ikke er andet lovligt behandlingsgrundlag, jf. litra b.

Det vil være svært at gennemføre nogen meningsfuld journalistisk virksomhed i bred forstand, hvis de mange regler i persondataretten skal efterleves, hvilket er baggrunden for undtagelsen i GDPR art. 85.

De danske undtagelser er pt. bygget op på en ikke helt overbevisende måde. På den ene side undtages al persondatabehandling i journalistisk øjemed efter DBL § 3, stk. 8 (med undtagelse af GDPR art. 28 og 32 og hele kapitel VIII, der ikke undtages). Dette er ikke i god overensstemmelse med GDPR art. 85, der lægger op til, at forordningens enkelte kapitler vurderes i forhold journalistisk virksomhed. I dansk ret er der ikke foretaget nogen sådan systematisk gennemgang, og den brede undtagelse kan netop derfor være for bred.[44] På den anden side er de danske regler for mediedatabaser, hvilket i realiteten vil sige stort set alle onlinemedier, knyttet til medieansvarsloven, ligesom loven indeholder krav om løbende sletningsovervejelser. Her synes undtagelsen at være

42. Lovteknisk er videregivelse til politiet en tungtvejende interesse efter databeskyttelseslovens § 8, stk. 4, og i tv-overvågningsloven er det præciseret, at der kan ske videregivelse til politiet, jf. § 4 c, stk. 3.
43. Se også Sandfeld Jakobsen & Schaumburg-Müller, »Retten til at blive glemt – og forholdet til medierne og informationsfriheden«, *Juristen* 2015, s. 176-186.
44. Se nærmere Jakobsen & Schaumburg-Müller, op.cit. (note 16).

for snæver, og kravene til medierne for stramme. (Se nærmere nedenfor afsnit 5).

Den, hvis personlige data behandles – »den registrerede« – har som udgangspunkt ret til:
– at blive orienteret om behandlingen
– på forespørgsel at blive orienteret (indsigtsret)
– at få slettet eller rettet forkerte eller ulovlige registreringer.

4. Særligt om personbilleder

Selve det at tage et billede af en person er en persondatabehandling. Det samme gælder enhver videregivelse, hvad enten det er til offentligheden eller blot til en enkelt. Muligheden for en sådan persondatabehandling, altså at tage eller videregive et personbillede, falder overordnet i to grupper: For det *første* kan aktiviteten helt være undtaget persondatarettens regler, og for det *andet* kan aktiviteten være lovlig i henhold til en bestemmelse i databeskyttelsesloven.

Den første gruppe er omtalt ovenfor i afsnit 2, og i det følgende ses nærmere på, hvad dette betyder for personbilleder.

Efter DBL § 3, stk. 1, finder persondataretten ikke anvendelse, hvis det vil stride mod ytrings- og i informationsfriheden. Denne undtagelse har ikke den store betydning for billeder. EMD lægger netop vægt på, at offentliggørelse af personbilleder kan være mere indgribende, jf fx Gourguenidze v Georgien 17. oktober 2006, hvor EMD fandt at omtalen af sagen – salg af en kendt forfatters manuskript – havde offentlig interesse og dermed var beskyttet af art. 10, mens netop videregivelse af personbilledet ikke var relevant og derfor i strid med art. 8. Man kan ikke afvise, at § 3, stk. 1, kan finde anvendelse i særlige tilfælde, hvor det er vigtigt for dokumentationen af et offentligt interessant spørgsmål at videregive et personbillede.[45] I sådanne tilfælde vil man normalt kunne bruge afvejningsreglen i GDPR art. 6, stk. 1, litra f, der taler om »legitime interesser«.

Undtagelsen efter GDPR art. 2, stk. 2, litra c, og DBL § 1, stk. 2, om den rent personlige og familiemæssige behandling, er formentlig den, der giver flest problemer i praksis. Hvorvidt der er tale om en sådan personlig aktivitet, skal vurderes i forhold til hver enkelt behandling. Det at tage billeder til egen

45. Sammenlign med STL kapitel 27, hvor det i særlige tilfælde kan være berettiget at tage billeder af personer på ikke frit tilgængeligt sted og at videregive private billeder. Se nærmere kap. 3, afsnit 2.6.

samling vil normalt være uden for persondatarettens rækkevidde, og det samme gælder videregivelse til venner og familie. Videregivelse til en større offentlighed vil næppe være »rent personlig«, men som nævnt ovenfor afsnit 2.2 er det uklart, hvor meget der kan lægges på nettet og fortsat være rent personligt. Bruger man billeder, der er optaget lovligt i persondatarettens forstand, i reklamer, i politisk øjemed eller som led i journalistisk virksomhed, er videregivelsen klart ikke rent personlig.

Bortset fra samtykke vil afvejningsreglen i art. 6, stk. 1, litra f, formentlig være den, der oftest kommer i spil. Her sondrede Datatilsynet tidligere mellem portrætbilleder og situationsbilleder, hvor offentliggørelse af portrætbilleder normalt kun kunne tillades med de afbildedes samtykke, mens situationsbilleder normalt uden videre var tilladt, dog med en del undtagelser. Datatilsynet har imidlertid forladt denne position,[46] og det hedder nu: »Ved vurderingen af, om der kan ske offentliggørelse af et billede på baggrund af en interesseafvejning, kommer det bl.a. an på karakteren af billedet, herunder hvor og hvorfor billedet er taget, i hvilken sammenhæng billedet indgår, og hvad der er formålet med offentliggørelsen. Det er afgørende, at de personer, der er på billedet, ikke med rimelighed kan føle sig udstillet, udnyttet eller krænket …«.[47] Datatilsynet synes at lægge sig op ad de kriterier, som Den Europæiske Menneskerettighedsdomstol (EMD) har udviklet i forbindelse med videregivelse af personbilleder:[48]

– Er billedet med til at belyse et emne af offentlig interesse?
Et billede fra en offentlig begivenhed, en koncert, et sportsarrangement, en politisk begivenhed mv. har offentlig interesse, mens det ikke har nogen offentlig interesse, at en person ser speciel ud eller at to personer er kærester mv.

– Er der tale om en kendt person?
En kendt person må tåle mere. Dette betyder ikke, at kendte personer helt frit kan afbildes, men det betyder, at personer, hvis billede i forvejen er kendt, ikke helt i samme grad har samme beskyttelsesbehov.

46. Sondringen var som udgangspunkt let at håndtere, men behæftet med en del usikkerhed og uklarhed. Og altså nu forladt.
47. *Datatilsynet*, https://www.datatilsynet.dk/emner/internet-og-apps/billeder-paa-internettet, tilgået 14. oktober 2020.
48. Se fx von Hannover v Tyskland nr. 2 12.2.2012 GC, pr. 108-113.

– Hvad er fortælles med billedet?

Der er forskel på et billede, der viser en begejstret tilskuer, og et billede, der viser en surt udseende person eller en person, der er i gang med mere private forehavender.

– Form, indhold og konsekvenser

Dette er en noget bred kategori, men især vurdering af konsekvenser af en offentliggørelse kan være vigtige. Bliver den afbildede beskrevet som den grimmeste eller mest underlige, taler dette for beskyttelse af den afbildede i hvert fald imod offentliggørelse og anden behandling af billedet.

– Forholdene ved selve fotograferingen

Er der tale om egentlig paparazzi-fotografering, hvor en person forfølges, taler dette for en beskyttelse af den afbildede. Det samme gør, hvis den afbildede befinder sig et sted, hvor man ikke normalt regner med at blive fotograferet, en øde strand fx Omvendt hvis den afbildede befinder sig et sted med mange mennesker. Eftersom næsten alle har et kamera ved hånden, bliver der fotograferet meget, og på offentlige steder med en del mennesker må man påregne at kunne blive fotograferet.

Personbilleder er personoplysninger.
Behandling af personbilleder kan bestå i tage et fotografi, lagre det, videregive det, offentliggøre det, slette det mm.
Behandling som led i rent personlig eller familiemæssig aktivitet eller som udelukkende finder sted i journalistisk øjemed er undtaget, og det gælder også behandling af personbilleder.
Hvis behandlingen ikke er undtaget, skal man finde en relevant bestemmelse, der giver ret til hver enkelt behandling. Samtykke vil jævnligt være relevant. Det samme gælder afvejningsreglen, især hvor der er tale om selvoffentliggørelse.

5. Massemedieinformationsdatabaseloven

Ifølge § 1 i lov om massemediers informationsdatabaser (herefter mediedatabaseloven eller MDL)[49] gælder loven »for informationsdatabaser, der er massemedier, eller som drives i tilknytning til en eller flere virksomheder, der udgiver massemedier«. Et medie kan således i sig selv udgøre en database, hvilket formentlig er tilfældet for de almindelige massemediers hjemmesider, hvor der kan søges efter forskellige kriterier. Det er ikke tilstrækkeligt, at en database blot drives af et medie, databasen skal tillige have »forbindelse med formidling af nyheder og andre informationer«, § 2, stk. 2. En database, der ikke har en sådan forbindelse som fx et medies kundekartotek, er ikke omfattet af loven, hvilket indebærer, at behandling af persondata skal behandles efter persondatarettens regler.

Loven opererer med tre typer informationsdatabaser:

5.1. Uredigerede fuldtekstinformationsdatabaser

Den første kategori omfatter de databaser, der kun gengiver, hvad der allerede er offentliggjort i medier omfattet af medieansvarsloven. Disse såkaldte uredigerede fuldtekstdatabaser[50] er ikke omfattet af loven, jf. MDL § 1, stk. 2 og 3, og i øvrigt heller ikke af databeskyttelsesloven, jf. den tilsvarende undtagelse i DBL § 2, stk. 5 og 6. Meningen er, at dette stofs offentliggørelse allerede er underlagt straffeloven og medieansvarsloven mv. i og med den første offentliggørelse, hvilket bl.a. indebærer, at en forurettet som udgangspunkt altid vil kunne finde en at rette sit krav imod.

5.2. Redaktionelle informationsdatabaser

Den anden kategori udgøres af interne databaser, de såkaldte redaktionelle informationsdatabaser, reguleret i MDL §§ 3-5. Ideen er, at redaktioner og journalister skal kunne anvende databaser med personoplysninger uden hensyntagen til de mange persondataretlige regler. Kendetegnende for en redaktionel database er således, at den ikke er tilgængelig for andre end mediets journalister og redaktionelle medarbejdere, og at den ikke må bruges til andet end journalistisk eller redaktionelt arbejde. Til gengæld for kravet om kun intern brug er der intet forbud mod behandling af selv følsomme personoplysninger og intet krav om indsigtsret el.lign. Kategorien er omfattende og dækker over såvel tekstbehandling, redigeringsprogrammer som egentlige databaser, og selv de

49. Lov 430/1994 som ændret ved lov 429/2000 og 433/2000.
50. Bet. 1233/1992 om pressens informationsregistre, s. 66.

notater, en journalist gør sig på sin pc, er også omfattet.[51] For at høre under denne kategori skal en række forudsætninger være opfyldt:

- De skal »alene drives som led i journalistisk eller redaktionelt arbejde«, MDL, § 2, stk. 3.
- De skal endvidere drives »med henblik på offentliggørelse i et massemedie«, § 2, stk. 3, og dette massemedie skal være omfattet af medieansvarsloven, MDL § 2, stk. 1. Heri ligger, at journalistisk arbejde med henblik på offentliggørelse ad andre kanaler, fx bøger eller udenlandske medier, formentlig ikke kan benytte sig af disse gunstige regler, men skal følge reglerne i databeskyttelsesloven.
- Databasen skal være anmeldt til Datatilsynet, jf. § 3. Hvert medie behøver kun at anmelde én gang, hvad angår redaktionelle databaser. Uden anmeldelse gælder persondatarettens regler.
- Efter § 4, stk. 1, må en redaktionel informationsdatabase ikke være tilgængelig for andre end massemediets journalister og redaktionsmedarbejdere, og den må ikke benyttes til andet end journalistisk eller redaktionelt arbejde, jf. § 4, stk. 2.
- Efter § 5 skal der »træffes de fornødne sikkerhedsforanstaltninger mod, at uvedkommende får adgang til en redaktionel informationsdatabase«. Det er ikke efter loven klart, hvad der kan betegnes som fornødne sikkerhedsforanstaltninger. Selvom DBL § 3, stk. 4, er formuleret således, at art. 28 og 32 ikke gælder for disse databaser – i modsætning til anden journalistisk aktivitet, DBL § 3, stk. 7 og 8 – må »fornødne sikkerhedsregler« forstås i overensstemmelse med GDPR art. 32, der både er mere eksplicit og mere opdateret.[52]
- Der skal træffes foranstaltninger med henblik at sikre mod (de mange) uvedkommendes adgang og mod, at informationsdatabasen benyttes til uvedkommende formål, jf. § 5. Bemærk, at en mobiltelefon typisk har en database med relevante telefonnumre. Dette kan udgøre en redaktionel database, og for at have beskyttelse efter mediedatabaseloven, må man bl.a. sørge for, at ikke alle kan få adgang.

51. Bet. 1233/1992, s. 67.
52. Der kan selvfølgelig opstå spørgsmål om, hvorvidt en dansk eller en EU-retlig bestemmelse har forrang, se fx Højesterets dom af 6. december 2016 (Ajos). I nærværende situation med spørgsmålet om tilstrækkelige sikkerhedsforanstaltninger forekommer det oplagt at fortolke i overensstemmelse med nyere regler, ikke mindst henset til at området teknisk har udviklet sig markant siden 1995, da mediedatabaseloven trådte i kraft.

Reglerne om redaktionelle informationsdatabaser er ganske fornuftige og velbegrundede. Redaktionelle medarbejdere kan let undgå persondatarettens mange regler, udelukkende på betingelse af anmeldelse og på overholdelse af grundlæggende sikkerhedskrav, der som nævnt nu må fortolkes i lyset af GDPR art. 32.

Kritisk kan det påpeges, at journalistisk her ikke forstås bredt, som krævet efter EU-retten, men snævert er knyttet til medieansvarsloven.

Stort set alle journalister opererer med databaser, fx på pc'er, iPads, mobiltelefoner mv. Stort set alle journalisters databaser involverer behandling af persondata

For at sådanne databaser kan være lovlige, kræves:

- at mediet er omfattet af medieansvarsloven,
- at mediets databaser er anmeldt til Datatilsynet,
- at databasen ikke er tilgængelig for andre end redaktionelle medarbejdere, og
- at der er foretaget fornødne sikkerhedsforanstaltninger.

5.3. Andre offentligt tilgængelige informationsdatabaser

Den tredje kategori udgøres af »offentligt tilgængelige informationsdatabaser«, reguleret i MDL kap. 3, §§ 6-11a. Langt de fleste netmedier vil udgøre en informationsdatabase i lovens forstand, og for at være omfattet af lovens og dennes særlige regler skal følgende betingelser være opfyldt:

- Databasen skal være tilgængelig for enhver på almindelige forretningsvilkår, jf. § 6, stk. 1. Der kan således uden problemer sættes vilkår, fx om betaling, men adgangen må ikke være begrænset til en bestemt personkreds fx i et intranet.
- Databasen skal endvidere være anmeldt både til Pressenævnet og til Datatilsynet med angivelse af en ansvarlig, jf. § 6, stk. 1. Manglende opfyldelse heraf må medføre, at databasen er underlagt persondatarettens regler, medmindre den kan falde ind under én af de to øvrige kategorier.

Tidligere var der nogen uklarhed med hensyn til, om en informationsdatabase både kunne være et medie omfattet af medieansvarsloven og en offentligt tilgængelig informationsdatabase efter MDL kap. 3. Problemet er nu løst ved lov 503/2018 § 7, nr. 1, der ophæver MDL § 6, stk. 2. Herefter er der ingen tvivl om, at et medie, der samtidig er en database, både kan være omfattet af medieansvarsloven og mediedatabaseloven, naturligvis under den forudsætning, at mediet/databasen er anmeldt til henholdsvis Pressenævnet og Datatilsynet)

De offentligt tilgængelige infodatabaser er reguleret på en måde, der dels ligner reguleringen af andre medier, dels har visse fællestræk med persondataretten, fx med hensyn til sletning, ajourføring mv.:

Efter § 8, stk. 1, må databasen ikke indeholde informationer, der ikke lovligt kan offentliggøres i et medie, og efter § 8, stk. 2, gælder det samme for informationer, hvis offentliggørelse ville være i strid med god presseskik.

Da der er tale om en database med i princippet ubegrænset lagringstid, bestemmer § 8, stk. 3, endvidere, at oplysninger om »rent private forhold« som udgangspunkt kun må lagres i tre år fra begivenheden, eller hvis denne ikke kan stadfæstes, fra lagringen. Kravet om sletning gælder dog ikke, »hvis der består en sådan interesse i, at de pågældende informationer er offentligt tilgængelige, at hensynet til den enkeltes interesse i, at informationerne slettes, findes at burde vige for hensynet til informationsfriheden«. For fx politikere, skuespillere, idrætsstjerner osv. kan det derfor forekomme rimeligt at opbevare oplysninger om fx politiske og strafbare forhold ud over de tre år, bl.a. fordi der fortsat er en nyhedsmæssig interesse knyttet hertil.

De berørte har i øvrigt særlige *rettigheder*, når det drejer sig om offentligt tilgængelige informationsdatabaser, herunder bl.a. ret til på anmodning at få oplyst, hvem der er dataansvarlig, at kræve sletning, rettelse eller ajourføring, hvis oplysningerne er urigtige eller vildledende, at kræve genmæle efter medieansvarslovens regler samt at kræve indsigt i eventuelle oplysninger i basen om én selv.

Sådan som loven er formuleret, vil langt de fleste netmedier være en »offentligt tilgængelig informationsdatabase«, der kan anmeldes til både Pressenævnet og Datatilsynet. Endvidere skal anmeldte netmedier løbende vurdere, om der er grund til at slette oplysninger efter tre år og tage stilling til anmodninger om sletning, rettelser eller ajourføring. Pressenævnet skal tage stilling i tilfælde af uenighed mellem netmediet og den registrerede.

I realiteten er der næppe mediedatabaser, der opfylder disse betingelser, og reguleringen er ikke optimal.

For det *første* er det upraktisk, at mediedatabaser efter denne lov er forpligtet til løbende at vurdere alle tre år gamle personoplysninger. Næppe noget medie foretager faktisk en sådan vurdering, og det er et temmelig uoverkommeligt og omkostningskrævende arbejde.

For det *andet* foreskrives en ret til sletning også og især for korrekte oplysninger. Mediedatabaseloven opererer ikke med andre muligheder, såsom afindexering eller anonymisering, og man kan argumentere, at egentlig sletning altid er et uforholdsmæssigt indgreb i informationsfriheden, selvom det klart

ikke var, hvad der blev lagt op til ved lovens indførelse. Der ses ikke i afgørelsespraksis at være sager, hvor en offentligt tilgængelig informationsdatabase er pålagt sletning efter mediedatabaseloven.

5.4. Klager

Pressenævnet er kompetent som klageorgan vedrørende mange, men ikke alle rettigheder efter mediedatabaseloven, jf. i det hele lovens kapitel 4.

Pressenævnets afgørelser kan ikke indbringes for anden administrativ myndighed, jf. § 15, men må indbringes for domstolene,[53] og manglende efterkommelse af Pressenævnets kendelser kan medføre straf, jf. MDL § 16, helt svarende til ordningen efter medieansvarsloven.

Indtil videre synes Pressenævnet kun at have afsagt få kendelser i henhold til mediedatabaseloven, og Pressenævnet har ikke i nogen sager pålagt egentlig sletning.

6. Tv-overvågning

6.1. Hvad er tv-overvågning?

Tv-overvågning er reguleret af tv-overvågningsloven (TVOL),[54] der væsentligst, men ikke udelukkende, regulerer retten til overhovedet at foretage tv-overvågning. I det omfang overvågningen involverer behandling af personoplysninger, gælder tillige databeskyttelsesloven og forordningen, jf. DBL § 2, stk. 4.

Hvad tv-overvågning er i lovens forstand, bestemmes i TVOL § 1, stk. 2, som her citeres i sin helhed:

> Ved tv-overvågning forstås vedvarende eller regelmæssigt gentagen personovervågning ved hjælp af fjernbetjent eller automatisk virkende tv-kamera, fotografiapparat eller lignende apparat. Lovens regler om tv-overvågning finder tilsvarende anvendelse på opsætning af sådant apparat med henblik på overvågning.

Dette betyder for det *første*, at apparater, der opsættes fx for at se, hvordan det står til med stærefamilien i den opsatte stærekasse, ikke er omfattet af loven. Hvis man opsætter overvågning for at beskytte sin husdyr mod ulve, vil dette

53. Bemærk U 2003.71 H. Højesteret afviser sag anlagt mod Pressenævnet (der i sin kendelse ikke havde fundet, at der var handlet i strid med god presseskik) og henviser til søgsmål mod det pågældende medie.
54. Lbkg. 1190/2007 som ændret ved lovene 713/2010, 422/2011, 736/2014, 1728/2016 og 506/2018.

heller ikke være omfattet af tv-overvågningsloven. I tilfælde af, at et menneske kommer med på optagelsen, må det overvejes, om der herefter kan være tale om en persondatabehandling. Her skal man være opmærksom på GDPR art. 2, stk. 2, litra c, hvorefter en fysisk persons behandling som led i rent personlige eller familiemæssige aktiviteter ikke er omfattet af persondataretten. Er der tale om overvågning foretaget af en juridisk person, dvs. en virksomhed, en organisation eller en institution, er optagelsen omfattet af persondataretten under den selvfølgelige forudsætning, at der overhovedet optræder personer på optagelserne. Det samme gælder, hvis optagelsen ikke kun dækker privat område, men tillige inddrager offentligt område. Det kom EU-Domstolen frem til i C-212/13 Frantisek Rynes, hvor optagelser af egen indgang, der tillige fik noget af fortovet med, ikke ansås for undtaget den dagældende regulering. Dette må også efter de nye regler være gældende: Hvis man overvåger et offentligt tilgængeligt sted – eller andres private steder – er der ikke tale om en rent personlig eller familiemæssig aktivitet.

For det *andet* indebærer § 1, stk. 2, at der skal være tale om automatisk optagelse. En person, der fotograferer rigtig meget, bliver ikke omfattet af tv-overvågningsloven, men af bl.a. straffelovens regler om fotografering, især STL § 264a. Omvendt behøver tv-overvågningen ikke foregå konstant. Det er tilstrækkeligt, at den foregår regelmæssigt, fx med billeder op til hver halve time, jf. U 2005.2979V (Læsø havn). Det er heller ikke en betingelse, at der samtidig foretages optagelse (lagring), idet kameraovervågning med monitorer også er omfattet.

For det *tredje* er selve opsætningen af et kamera med henblik på overvågning omfattet af forbuddet, jf. § 1, stk. 2, 2. pkt.

Hvorvidt lydoptagelse er omfattet, er næppe ganske klart. Efter den tidligere lov blev det antaget af tv-overvågning kun angik det visuelle.[55] Nu regulerer § 4c imidlertid efter sin ordlyd både billed- og lydoptagelse, og det mest nærliggende må være at antage, at det så gælder hele loven og ikke kun den enkelte paragraf. Den praktiske virkning er ikke af stor betydning. Hvis man fx opsætter lydoptagelsesudstyr for at fange en solsorts sang, vil dette ikke være omfattet af tv-overvågningsloven, jf. kravet om »personovervågning«. Hvis der i optagelsen kommer (genkendelige) menneskestemmer med, må enhver efterfølgende behandling vurderes efter persondataretten. Hvis man derimod opsætter et apparat til at optage andres samtaler, må dette skulle følge kravene i tv-overvågningsloven. Endvidere bemærkes, at lydoptagelse uden egen deltagelse normalt vil være strafbar efter STL § 263, stk. 1, nr. 3.

55. Waaben og Nielsen (2015), s. 421.

6.2. Hvornår må man foretage tv-overvågning?

For private gælder det, at de ikke må foretage tv-overvågning af »gade, vej, plads eller lignende område, som benyttes til almindelig færdsel«, jf. TVOL § 1, stk. 1. Dette betyder, at man gerne må tv-overvåge på eget private område. Bemærk her, at der kan være andre begrænsninger, fx forbud mod at optage andres samtaler, STL § 263, stk. 1, nr. 3, og fotografering mv. af andre personer på ikke frit tilgængeligt sted, STL § 264a. Sidstnævnte bestemmelse kriminaliserer også iagttagelse ved hjælp af et apparat. Den situation, der forelå i EMD Söderman v Sverige 12.11.2013 [GC], hvor en stedfar havde sat et kamera til at optage steddatteren i badeværelset, vil således efter dansk ret ikke være omfattet af tv-overvågningsloven, men nok af straffeloven.[56]

Endvidere er der i § 2 en længere række specifikke undtagelser til forbuddet mod privates tv-overvågning af offentligt sted. Dette gælder fx erhvervsmæssig overvågning af overdækkede butiksområder, hæveautomater og egne facader mv. og under de i loven nærmere fastsatte betingelser.

Private skal normalt skilte, hvis der foretages tv-overvågning af områder med almindelig adgang og af arbejdspladser, jf. TVOL § 3, stk. 1.

Offentlige myndigheder må efter tv-overvågningsloven gerne foretage tv-overvågning – normalt med skiltning, jf. § 3a – men andre love mv. skal naturligvis overholdes, herunder også forvaltningslovens regler, inklusive almindelige sagsbehandlingsregler og normer for god forvaltningsskik. Hertil kommer persondata- og strafferettens regler. Det ligger uden for nærværende fremstilling at give et mere indgående kendskab til de forskellige regler og de forskellige aktører. Der henvises til lovens til tider detaljerede bestemmelser og til speciallitteraturen.

6.3. Hvad må man bruge optagelser til?

Den videre behandling af personoplysninger reguleres af især § 4 c, der i stk. 1 bestemmer, at billed- og lydoptagelser optaget i kriminalitetsforebyggende øjemed – hvilket er tilfældet for langt det meste tv-overvågning – kun må videregives, 1) hvis der er samtykke fra de(n) registrerede, 2) hvis det følger af anden lov, eller 3) hvis videregivelsen sker til politiet i kriminalitetsforebyggende øjemed. Dette betyder, at videregivelse til medier ikke er tilladt, ligesom det ikke vil være tilladt at uploade optagelserne på nettet, heller ikke selvom selve optagelserne er private og gengiver et (muligt) indbrud, jf. DT 2007-631-0020 af 5.9.2007. Bemærk her, at mens mediers brug typisk vil være undtaget fra persondataretten, jf. DBL § 3, stk. 4-8, (omtalt ovenfor i afsnit 2.3), gælder

56. Problemet efter svensk ret var, at et sådant forhold ikke var kriminaliseret, hvilket EMD fandt udgjorde en krænkelse af art. 8.

der ikke nogen tilsvarende undtagelse i tv-overvågningsloven. Dette må indebære, at også mediers videregivelse af tv-overvågningsbilleder er strafbar efter TVOL § 5, stk. 2, jf. § 4c. At medierne som følge af flytningen kan ifalde et strafansvar, var muligvis ikke tilsigtet, eftersom formålet blot var at videreføre reglerne.[57] Under alle omstændigheder skal også TVOL § 4c, stk. 1, fortolkes i overensstemmelse med EMRK art. 10, og i hvert fald i princippet kan tænke sig situationer, hvor det ville straffrit for et medie at videregive et overvågningsbillede

Med § 4c er tillige tilladt en ordning, hvorefter erhvervsdrivende kan dele billeder af (formodede) gerningsmænd. Der er dog en række betingelser knyttet hertil: der skal være tale om grovere kriminalitet (af »ikke bagatelagtig karakter«, som det hedder i stk. 2, nr. 1, der skal være foretaget en anmeldelse af den kriminelle handling, der skal være grund til at tro, at de pågældende vil foretage en »ligeartet kriminalitet« mod kredsen af de erhvervsdrivende, og delingen må kun foregå inden for et lukket netværk, hvor få har adgang, jf. stk., nr. 1-4. Optagelserne skal som udgangspunkt slettes efter 30 dage, § 4c, stk. 4 og 5.

Anden behandling af persondata end videregivelse af optagelser i kriminalitetsforebyggende øjemed, § 4c, og behandling af optagelser fra de særlige områder, § 4 d (som jf. ovenfor ikke er behandlet her), behandles efter persondatarettens øvrige regler, herunder GDPR art. 5 om principper for behandling af personoplysninger (se nærmere, om end kort ovenfor afsnit 3 og særskilt om personbilleder afsnit 4). Som eksempel har Datatilsynet i en konkret sag fundet, at tv-overvågning i et kollegiums fælleskøkken ikke opfyldte disse grundlæggende betingelser, jf. DT 2007-219-0043 af 11.1.2008. Det bemærkes, at Datatilsynet ikke i sagen tager stilling til anden lovgivning, herunder tv-overvågningsloven, der næppe gælder i et fælleskøkken, jf. »gade, vej, plads eller lignende område, der benyttes til almindelig færdsel«, jf. TVOL § 1, stk. 1.

57. Se Justitsministerens fremsættelse af lovforslag L 205 21. marts 2018