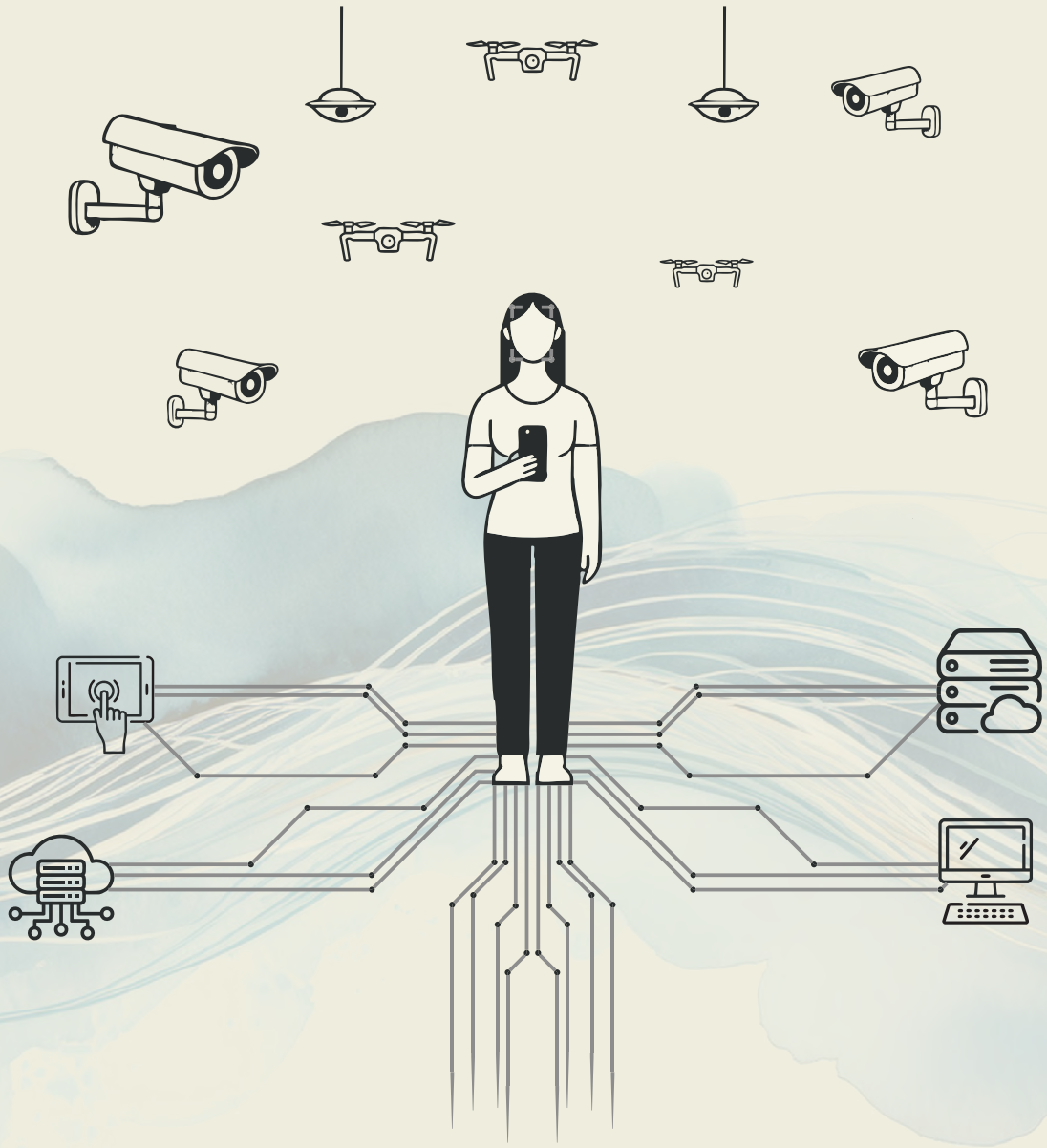
Udvalget for Digitalisering og It 2024-25
DIU Alm.del - Bilag 58
Offentligt

JUSTITIA

DANMARKS UAFHÆNGIGE
JURIDISKE TÆNKETANK



Rapport

Øget overvågning udfordrer retsstaten

Øget overvågning udfordrer retsstaten

Af Ditte Yde Amsnæs og Birgitte Arent Eiriksson. Gennemlæst og kommenteret af eksterne eksperter på området.

ISBN: 978-87-972489-6-6

Justitia - Danmarks uafhængige juridiske tænketank
Vesterbrogade 69D, 1. sal. th. 1620 København
www.justitia-int.org
info@justitia-int.org

Justitia er Danmarks eneste juridiske tænketank, der alene har fokus på retssikkerhed og frihedsrettigheder. Justitias formål er gennem analyser af høj faglig kvalitet og fremsættelse af konkrete juridiske løsningsforslag at påvirke den offentlige og politiske dagsorden med henblik på at fremme en politisk kultur, hvor disse værdier nyder den nødvendige respekt.

Rapporten er blevet til med støtte fra FRi Puljen.

Indhold

"Konstant overvågning sikrer borgernes bedste opførsel."

Larry Ellison, medstifter af softwarefirmaet Oracle, 2024.

1 Resume

Den teknologiske udvikling, digitaliseringen og et politisk ønske om øget tryghed, kontrol og besparelser har ført til en markant udvidelse af myndigheders overvågning af borgerne. Det udfordrer balancen mellem på den ene side sikkerhed og effektivitet og på den anden side beskyttelsen af grundlæggende frihedsrettigheder.

Denne rapport undersøger udviklingen i overvågningstrykket i Danmark med særligt fokus på myndigheders brug af TV-overvågning, indsamling af digitale data og systematisk datasamkøring. Rapporten indeholder en analyse af de lovgivningsmæssige og menneskeretlige rammer, herunder retten til privatliv og beskyttelse af personoplysninger. Rapporten indeholder desuden en oversigt over de seneste ti års begivenheder, tiltag, og faktuelle forhold, der påvirker retten til privatliv og beskyttelse af personoplysninger.

Rapporten viser, at det offentlige rum overvåges markant mere end tidligere, og at myndighedernes muligheder for at overvåge for at 'fremme trygheden' eller af 'tryghedsskabende' grunde er blevet markant udvidet, uden det er blevet nærmere defineret, hvad der ligger i disse udtryk, og uden det kan dokumenteres at forebygge den kriminalitet, der angives som grund for overvågningen. Det rejser tvivl om legitimiteten af overvågningen. Samtidig bliver det meget vanskeligt at vurdere, hvornår en sådan overvågning er nødvendig, virksom og dermed proportional.

På samme vis bliver danske borgere udsat for markant mere dataovervågning end tidligere. Samtidig er rammerne for det myndighedsmæssige skøn til at vurdere, hvornår og hvilke oplysninger, der systematisk skal videregives og samkøres i kontroløjemed, i væsentlig grad blevet udvandet. Myndighederne kan derfor mere eller mindre frit beslutte, hvad der kan anses for nødvendigt for kontrolindsatsen. Det indebærer en markant øget adgang til at indhente, genanvende og samkøre oplysninger både internt og med oplysninger indhentet fra andre myndigheder, private virksomheder og offentligt tilgængelige kilder. Det sker til formål, som både omfatter kontrol, profilering, risiko-scoring og til udvikling af algoritmer og it-systemer.

Rapporten afdækker en række faktorer, som hver for sig og tilsammen påvirker intensiteten af statens overvågning af borgerne. Overordnet kan faktorerne anskues fra tre vinkler: 1) Den teknologiske udvikling, 2) den politiske vilje og 3) de retlige rammer.

Den teknologiske udvikling har uden tvivl haft afgørende indflydelse på overvågningens intensitet og omfang. Ny teknologi øger sporbarheden og giver nye muligheder for at sammenstille og profilere borgerne. Det muliggør en endnu mere intens, men ikke nødvendigvis mere ressourcekrævende overvågning og kontrol, da teknologien samtidig bliver billigere og mere tilgængelig.

Den **politiske vilje** styrer integrationen af ny teknologi i myndigheders kontrolindsats, f.eks. ved øget kameraovervågning og digitalisering. Effektivitetskrav og hensynet til borgernes sikkerhed har

gennem årtier være drivende for at igangsætte nye initiativer, som øger overvågningen i samfundet. Senest ses et stærkt incitament til at investere i kunstig intelligens, der intensiverer overvågningen.

Udviklingen af **de retlige rammer** er i særlig grad kendetegnet ved, at myndighedernes skøn i forhold til, hvornår der kan anvendes overvågning, er blevet stadig bredere. Dermed er det blevet mere uklart for borgerne, hvornår de kan blive udsat for overvågning.

I et demokratisk samfund kan det sagtens være legitimt at skrue op for myndighedsbeføjelserne, men beskyttelsen af borgernes retssikkerhed og grundlæggende rettigheder er nødt til at følge med. De udgør selve grundstenen i en moderne, demokratisk retsstat. Derfor er det er også meget risikabelt at file på disse principper og rettigheder, uanset hvor gode de politiske hensigter er. Det kan hurtigt komme til at sætte tilliden til de offentlige myndigheder over styr, hvilket er yderst problematisk i en retsstat baseret på demokratiske værdier, hvor borgerne betragtes som frie og ligeværdige individer.

Ovenstående uddybes i rapportens delkonklusioner og afsluttende sammenfattende konklusion.

Anbefalinger

Anbefaling 1 - Kommission for Privatlivets Fred: Der skal nedsættes en kommission, som skal vurdere rammer og generelle vilkår for beskyttelsen af privatlivets fred i Danmark. Kommissionen skal også overveje, hvordan det kan sikres, at det samlede overvågningsomfang indgår i overvejelserne, når nye overvågningstiltag initieres og foreslås.

Anbefaling 2 - Overblik over det samlede overvågningsomfang: Der skal udpeges en central instans, som løbende kan skabe overblik over myndighedernes samlede overvågning af borgerne.

Anbefaling 3 - Klart retsgrundlag og sikring af demokratisk legitimation: Alle fagministerier skal forpligtes til at sikre, at alle fremtidige og eksisterende overvågningstiltag beskrives og reguleres særskilt med et klart retsgrundlag.

Anbefaling 4: Grundig lovgivningsproces: Alle lovforslag, som indeholder overvågningstiltag, skal ledsages af ensartede og strukturerede konsekvensvurderinger til belysning af retssikkerheds- og rettighedsmæssige konsekvenser, dataetiske overvejelser og en oversigt over allerede eksisterende overvågningstiltag på det pågældende område. Lovforslag om overvågningstiltag skal altid behandles i både Retsudvalget og det relevante fagudvalg.

Anbefaling 5 - Overvågningsetisk reflektionsværktøj: Der udarbejder et overvågningsetisk reflektionsværktøj, som skal være obligatorisk at anvende for myndighederne, når der overvejes tiltag og ny teknologi, der kan øge overvågning.

Anbefaling 6 - Evaluering af overvågningstiltag med fokus på proportionalitet: Øget fokus på grundig evaluering af, om formålet med overvågningen opnås, og at eksisterende overvågningstiltag ikke udvides uden forudgående evaluering af anvendelse og udbytte mm.

Anbefaling 7 - Øget gennemsigtighed: Der skal sikres et øget oplysningsniveau overfor borgerne, både når det gælder dataovervågning og videoovervågning,

Anbefalinger uddybes i afsnit 9

2 Indledning og rapportens fokus

Den første lov, som integrerede begrebet *overvågning*, var lov om forbud mod privates tv-overvågning fra 1982, der oprindeligt tog udgangspunkt i et generelt forbud mod videoovervågning på offentligt tilgængeligt område. Til dette udgangspunkt blev oprindeligt kun fastsat enkelte, klart definerede undtagelser.

Overvågning blev dengang anset for at være et særdeles invasivt indgreb i privatlivets fred, som kun under helt særlige omstændigheder kunne tillades. I det lovforberedende udvalgs betænkning var det opfattelsen, at videoovervågning i sig selv kunne virke utryghedsskabende for den almindelige borger. Det blev anset som en grundlæggende rettighed at kunne gå i fred på offentligt tilgængelige områder uden at risikere at blive filmet eller endda optaget til senere brug.[1] Bestemmelserne i loven byggede på den opfattelse, at befolkningen skulle "*beskyttes over for udspionering, som man ikke var indstillet på at tage sig i agt for*".[2] Videoovervågningsudstyr var samtidig specialudstyr, som var forbeholdt de få.

Siden da har teknologien og holdningen til overvågning udviklet sig. Ny teknologi øger konstant søgbarheden og mulighederne for at kombinere billedmateriale og andre personlige oplysninger og indebærer derfor en markant øget systematisk og indgribende dataanvendelse. Samtidig kan AI-baserede sporingsteknikker som ansigtsgenkendelsesteknologi, tastemønstergenkendelse og ganggenkendelse gøre det muligt konstant at masseovervåge, følge, identificere og påvirke enkeltpersoner og dermed også påvirke deres moralske og psykologiske integritet.[3] Selvom databeskyttelsesmyndighederne mener, at brug af ansigtsgenkendelsesteknologi er meget indgribende og kun bør anvendes med meget stor varsomhed af retshåndhævende myndigheder,[4] viser en ny europæisk undersøgelse, at tre ud af fire europæere bakker op om politiets og efterretningstjenesternes brug af kunstig intelligens (AI) og ansigtsgenkendelsesteknologi.[5]

En ny fælles rapport fra tre skandinaviske menneskerettighedsinstitutter[6] sætter bl.a. fokus på danskeres holdning til overvågning. Rapporten viser, at 55 pct. af de adspurgte synes, at kameraer på offentligt sted får dem til at føle sig tryggere, 26 pct. har ingen holdning til det, mens 15 pct. ikke føler sig tryggere. Rapporten viser også, at 41 pct. af de adspurgte ikke har noget imod overvågning af elektronisk kommunikation, hvis dette kan hjælpe myndighederne med at bekæmpe kriminalitet.

---

[1] Gräs, Motzfeldt og Tranberg (2008): Tv-overvågning anno 2008.
[2] Se punkt 5 i bemærkninger til lov nr. 151 af 12. marts 1982, Folketingstidende spalte 3831-3832 med bemærkninger til Forslag til lov om tv-overvågning.
[3] European Union Agency for Fundamental Rights, Facial recognition technology: Fundamental rights considerations in the context of law enforcement, April 2019, s. 23.
[4] EDPB - Retningslinjer 5/2022 for anvendelse af ansigtsgenkendelsesteknologi på retshåndhævelsesområdet. Vedtaget den 26. april 2023.
[5] Artikel på CNBC: Three in four Europeans support use of AI by the police and military og artikel i Computerworld: Datatilsynet kalder ansigtsgenkendelse "meget indgribende" - men tre af fire borgere er trygge ved at lade politiet bruge teknologien - Computerworld.
[6] Exploring human rights awareness, attitudes and perception in Scandinavia (2024).

36 pct. bryder sig ikke om sådan overvågning, og 20 pct. har ikke taget stilling.[7] På trods af den overvejende positive indstilling til overvågning – i hvert fald hvis den antages faktisk at kunne hjælpe myndighederne med kriminalitetsbekæmpelse mv. – har en stor andel af de adspurgte i praksis ændret adfærd på grund af overvågning. F.eks. har 17 pct. afholdt sig fra at deltage i en debat på et socialt medie, og 20 pct. har betalt med kontanter frem for kreditkort, ligesom 10 pct. har afholdt sig fra at søge information online indenfor en række personfølsomme emner.[8]

Overvågningsområdet kalder mere end nogensinde på en omhyggelig afvejning af på den ene side de muligheder, som teknologien og digitaliseringen indebærer, og på den anden side de skadevirkninger, som kan følge med slækket respekt for grundlæggende frihedsrettigheder, f.eks. deltagelse i den offentlige debat. Retsstatsprincipper, frihedsrettigheder og dataetiske værdier bør spille en langt større rolle, når nye eller udvidende overvågningstiltag overvejes, så disse beslutninger ikke alene tages ud fra det enkelte – ofte helt legitime og hæderværdige formål – men også ses i sammenhæng med de mange andre tiltag, som i vidt omfang tegner et stadigt mere overvågeligt og i praksis også overvåget samfund.

Formålet med denne rapport er at kaste lys over de seneste års udvikling af overvågningstrykket i forhold til den danske stats kontrolorienterede overvågning uden for efterretningsområdet. Fokus er rettet mod den markant øgede videoovervågning i det offentlige rum og den øgede dataindsamling- og overvågning.[9] Samtidig inviterer rapporten til en mere retssikkerhedsorienteret og rettighedsmæssig funderet debat, når der skal overvejes nye tiltag, som vil øge presset på privatlivets grænser yderligere.

[7] Ibid. s. 27.
[8] Ibid. s. 29.
[9] Efterretningstjenesternes overvågning er således ikke behandlet i rapporten.

3 Overvågning og grundlæggende rettigheder

I dette kapitel redegøres der indledningsvist for begrebet overvågning i afsnit 4.1, hvorefter der i afsnit 4.2 redegøres for den overordnede menneskeretlige beskyttelse af de mest relevante frihedsrettigheder, der udfordres i forbindelse med overvågning. Hovedfokus er derfor på retten til privatliv og beskyttelse af personoplysninger. Kapitlet afsluttes med en delkonklusion i afsnit 4.3.

3.1 Begrebet overvågning

Der findes ikke nogen entydig definition af 'overvågning'. I ordbog over det danske sprog er overvågning defineret som *"at holde øje med noget eller nogen."* En juridisk definition af begrebet tv-overvågning findes i tv-overvågningsloven, som første gang så dagens lys i 1982 med følgende definition: "*Ved TV-overvågning forstås vedvarende eller regelmæssigt gentagen personovervågning ved hjælp af fjernbetjent eller automatisk virkende TV-kamera, fotografiapparat eller lignende apparat."* [10] I tv-overvågningslovens forarbejder fandtes det uden betydning for om der var tale om overvågning, om der skete billedoptagelse, eller om billederne blot blev vist på en tv-skærm eller lignende. Vægten var således lagt på det systematiske og vedvarende element.[11]

I takt med den omfattende digitalisering af vores samfund er der kommet flere nye typer teknologisk understøttet personovervågning til. Begrebet "overvågning" anvendes derfor i dag som en paraplybetegnelse for mange typer af mere systematiske og gentagne aktiviteter, der på varierende måde kan være indgribende i forhold til privatheden og privatlivets fred.[12] EU-Domstolen har f.eks. brugt betegnelsen overvågning i forbindelse med logning af teledata, idet domstolen udtalte, at den: "omstændighed, at lagringen af data og den efterfølgende anvendelse af dem finder sted, uden at abonnenten eller den registrerede bruger oplyses herom, er (…) egnet til at skabe en følelse hos de berørte personer af, at deres privatliv er genstand for konstant *overvågning*." [13] I den juridiske litteratur er overvågning bl.a. afgrænset som omfattende 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 er beskyttet efter lovgivningen, herunder EMRK, EU's charter om grundlæggende rettigheder og de databeskyttelsesretlige regler.[14]

I denne rapport anvendes begrebet overvågning i relation til teknologisk understøttet og systematisk personovervågning, som har et (myndighedsmæssigt) kontrollerende sigte. Det gælder både i forhold til overvågning i det fysiske rum i form af videoovervågning, og i relation til digital

[10] Jf. § 1, stk. 2 i lov nr. 278 af 9. juni 1982 om forbud mod privates tv-overvågning m.v.
[11] Gräs, Motzfeldt og Tranberg (2008): Tv-overvågning anno 2008.
[12] Blume (2014): Overvågning. Kan persondataretten gøre nytte?
[13] EU-domstolens afgørelse af 8. april 2014 (Forenede sager C-239/12 og C-594/12, præmis 37. Fremhævelse foretaget her.
[14] Langsted og Jakobsen (2014): I en højere sags tjeneste. Afvejningen mellem overvågning og privatliv i en retlig kontekst s. 42.

dataovervågning. Sidstnævnte omfatter for det første den aktive overvågning af data, der foretages, når myndigheder som f.eks. Udbetaling Danmark eller Skat via forskellige algoritmer og analytiske redskaber foretager systematisk og løbende samkøring af persondata fra både offentlige og private registre i kontroløjemed. For det andet omfattes iværksættelse af masseopbevaring (logning) af eksempelvis private teledata til efterfølgende brug som en slags overvågning-on-demand. Det er i den forbindelse ikke tillagt betydning, i hvilket omfang myndighederne vælger at gennemgå og anvende resultaterne af den databaserede overvågning.

3.2 Den menneskeretlige beskyttelse af frihedsrettigheder

Myndighedernes adgang til at overvåge borgerne begrænses af reglerne om beskyttelse af borgernes ret til privatliv og beskyttelse af personoplysninger. Idealet om beskyttelse af borgernes privatliv er udtrykt i den danske grundlovs § 72, som vedrører boligens ukrænkelighed og beskyttelse mod indgreb i meddelelseshemmeligheden. Derudover er retten til privatliv beskyttet i Den Europæiske Menneskerettighedskonvention (EMRK) og Europarådets forbundne konvention om beskyttelse af det enkelte menneske i forbindelse med elektronisk databehandling af personoplysninger.[15] Endelig er EU's Charter om grundlæggende rettigheder, som Danmark er forpligtet af i kraft af traktaten om den europæiske union, en central retsakt.[16] Disse overordnede regelsæt udgør den overordnede ramme for både dansk lovgivning om myndigheders overvågning af borgerne og den faktiske overvågning, der pågår.

3.2.1 EU´s Charter og EMRK om beskyttelse af retten til privatliv og personoplysninger

Beskyttelsen af retten til respekt for sit privatliv og familieliv, hjem og korrespondance findes i EMRK's artikel 8 og EU' s Charter artikel 7, som indholdsmæssigt svarer til hinanden.

[15] Den første version af Europarådets Konvention nr. 108 om beskyttelse af det enkelte menneske i forbindelse med elektronisk databehandling af personoplysninger er fra 1981. Konventionen, der er åben for tiltrædelse af lande uden for Europa, har kaldenavnet Konvention 108, og er ratificeret af Danmark, se bekendtgørelse nr. 59 af 16. maj 1991 af europæisk konvention af 28. januar 1981 om beskyttelse af det enkelte menneske i forbindelse med elektronisk databehandling af personoplysninger. Den reviderede udgave fra 2018, Convention for the protection of individuals with regard to the processing of personal data af 18. maj 2018, følger i vidt omfang EU's databeskyttelsesforordning. Denne opdaterede version kaldes Konvention 108+.

[16] Den Europæiske Unions Charter om grundlæggende rettigheder blev juridisk bindende i Danmark på traktatniveau den 1. december 2009, da Lissabon-traktaten trådte i kraft. Se EU's Charter med kommentarer (2014), s. 31. Charterets artikel 8 er ifølge de forklarende bemærkninger bl.a. baseret på den dagældende EU-regulering: Direktiv 95/46 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (persondatadirektivet), EMRK artikel 8 og Konvention 108.

Den Europæiske Menneskerettighedskonvention

Artikel 8

Stk. 1. Enhver har ret til respekt for sit privatliv og familieliv, sit hjem og sin korrespondance.

Stk. 2. 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.

Den Europæiske Unions charter om grundlæggende rettigheder

Artikel 7 - Respekt for privatliv og familieliv

Enhver har ret til respekt for sit privatliv og familieliv, sit hjem og sin kommunikation.

Bestemmelsernes kerneområde er at forhindre uhjemlet, vilkårlig og uforholdsmæssig indblanding i fysiske og juridiske personers liv og aktiviteter.[17] Fortolkningsreglerne i EU´s Charter sikrer, at betydningen og rækkevidden af de rettigheder, der er beskyttet i begge regelsæt, stemmer overens, dog således, at EU-retten kan indebære en mere vidtrækkende beskyttelse, end hvad der følger af EMRK.[18]

EU's Charter indeholder derudover en særlig beskyttelse af personoplysninger i artikel 8:

Artikel 8 i EU's Charter om grundlæggende rettigheder:

1. Enhver har ret til beskyttelse af personoplysninger, der vedrører den pågældende.
2. Disse oplysninger skal behandles rimeligt, til udtrykkeligt angivne formål og på grundlag af de berørte personers samtykke eller på andet berettiget ved lov fastsat grundlag. Enhver har ret til adgang til indsamlede oplysninger, der vedrører den pågældende, og til berigtigelse heraf.
3. Overholdelsen af disse regler er underlagt en uafhængig myndigheds kontrol.

I kraft af EU's Charter er artikel 8 en grundrettighed, som samtidig indebærer en positiv pligt for staten til at sikre behandling af oplysninger i overensstemmelse med de principper om rimelighed, udtrykkeligt formål og retsgrundlag og gennemsigtighed, som følger af bestemmelsen.[19] Om betydningen af artikel 8 for retten til privatliv har EU-domstolen flere gange udtalt, at statens pligt

[17] EU's Charter med kommentarer (2014), s. 123.
[18] EU's Charter artikel 52, stk. 3 og artikel 53.
[19] EU's Charter med kommentarer (2014), s. 123.

til at beskytte personoplysninger i medfør af charterets artikel 8, litra 1, har særlig betydning for retten til respekt for privatlivet, som fastslået i artikel 7.[20]

En lignende bestemmelse findes ikke i EMRK, men den generelle bestemmelse i EMRK artikel 8, der beskytter den intime privatsfære, hvor individet skal kunne være i fred for indgreb fra offentlige myndigheder, kan dog efter omstændighederne også omfatte offentlige myndigheders behandling af personoplysninger.[21] Det beror på den kontekst, hvori oplysningerne er blevet indsamlet og opbevaret, den måde de anvendes og behandles samt de herved opnåede resultater, om der konkret er tale om data med sådanne privatlivsaspekter, at de er omfattet af retten til privatliv. Den systematiske indsamling og opbevaring af personoplysninger i offentlige myndigheders registre kan i sig selv være tilstrækkelig til at aktualisere privatlivsbeskyttelsen. Tilsvarende gælder for udveksling af personlige oplysninger mellem offentlige myndigheder uden samtykke fra den berørte person.[22]

Retten til respekt for privatlivet henholdsvis beskyttelse af personoplysninger er dog ikke absolut. Efter fast praksis fra både Menneskerettighedsdomstolen og EU-domstolen kan staten gøre indgreb i de grundlæggende rettigheder, hvis tre betingelser er opfyldt: 1) indgrebet skal forfølge et legitimt formål, 2) det skal have en klar lovhjemmel, og 3) det skal kunne anses for at være nødvendigt og proportionalt i et demokratisk samfund.[23]

At indgrebet skal forfølge et legitimt formål, vil typisk ikke volde de store udfordringer, da en meget bred vifte af hensyn betragtes som legitime. Kravet om lovhjemmel indebærer både et krav om hjemmel i lov og et krav om en vis lovkvalitet, så indgrebet er tilstrækkeligt afgrænset og forudsigeligt.[24] Kravet om proportionalitet indebærer navnlig, at indgrebet skal være nødvendigt for at opnå det påtænkte resultat og udgøre det mindst mulige indgreb, der kan realisere formålet.[25] EU-domstolen har udtrykt det således: *"Enhver begrænsning i udøvelsen af de rettigheder og friheder, der anerkendes i charteret, skal være fastlagt i lovgivningen og respektere disse rettigheder og friheders væsentligste indhold, og der kan under iagttagelse af proportionalitetsprincippet kun indføres begrænsninger, såfremt disse er nødvendige og faktisk svarer til mål af almen interesse, der er anerkendt af Unionen eller et behov for beskyttelse af andres rettigheder og friheder."*[26]

3.2.2 Øvrige rettigheder og principper

Ud over retten til beskyttelse af privatliv og personoplysninger kan også andre menneskerettigheder blive påvirket, når staten overvåger borgerne. **Ytringsfriheden** og **forsamlingsfriheden** er centrale

[20] Se bl.a. præmis 53 i EUD af 8. april 2014, Digital Rights-dommen (forenede sager C-293/12 og C-594/12).
[21] Jf. bl.a. EMD-dommene S. og Marper mod Storbritannien, 2008, og Uzun mod Tyskland, 2010. Endvidere henvises til Den Europæiske Menneskerettighedskonvention med kommentarer af Peer Lorenzen m.fl., art. 1-9, 3. udg., s. 665 ff. og EU´s Charter om Grundlæggende Rettigheder med kommentarer af Jonas Christoffersen, 2014, s. 133.
[22] Den Europæiske Menneskerettighedskonvention med kommentarer af Peer Lorenzen m.fl., art. 1-9, 3. udg., s. 665-666 og 671.
[23] Jf. EMRK artikel 8, stk. 2, som udmøntet gennem domstolens praksis.
[24] Den Europæiske Menneskerettighedskonvention med kommentarer af Peer Lorenzen m.fl., art. 1-9, 3. udg., s. 764.
[25] Den Europæiske Menneskerettighedskonvention med kommentarer af Peer Lorenzen m.fl., art. 1-9, 3. udg., s. 764.
[26] EUD af 8. april 2014, Digital Rights-dommen (forenede sager C-293/12 og C-594/12), præmis 38.

rettigheder at have for øje i forbindelse med overvågning. I forhold til ytringsfriheden peger de i afsnit 2 refererede undersøgelser i retning af, at bevidsthed om, at man som borger er under konstant overvågning, er egnet til at virke adfærdsændrende. Der opstår i den forbindelse risiko for en *chilling-effekt* i forhold til, om individer tør eller ønsker at ytre sig i samfundsdebatten. Tilsvarende må antages at gælde for deltagelse i ellers lovlige demonstrationer. Det vil formentlig især gælde, hvis der i forbindelse med videoovervågning i det offentlige rum anvendes ansigtsgenkendelsesteknologi, ganggenkendelsesteknologi eller lignende.[27] Grunden til, at der også her kan opstå en *chilling-effekt,* er, at gruppeanonymitet er et nødvendigt aspekt af forsamlingsfriheden. Brugen af biometriske genkendelsesteknologier på videoovervågningsoptagelser kan modvirke denne form for anonymitet ved at identificere og registrere enkeltindivider i selv store menneskemængder. Sådanne konsekvenser af overvågning kan på sigt udgøre alvorlige barrierer for et velfungerende demokrati.[28]

Også **retten til ikke at blive diskrimineret** kan blive påvirket som følge af den øgede overvågning og forbundne dataindsamling.[29] Der er for det første historisk erfaring for, at visse typer oplysninger under ændrede politiske forhold er blevet genbrugt til systematisk diskrimination fra statens side, f.eks. oplysninger om etnisk oprindelse, religiøs overbevisning, seksuel orientering, politisk overbevisning, helbredsoplysninger mv. For det andet kan diskrimination i nutidens digitale forvaltning ske utilsigtet og skjult. Diskrimination kan bl.a. opstå som konsekvens af de valg – eller mangel på valg – der tages i forbindelse med design, testning og implementering af algoritmer anvendt som led i dataovervågning. Anvendelse af visse teknologier, såsom kunstig intelligens, indebærer samtidig, at det ikke altid er muligt at forstå beslutningsvejene i sådan et system.

Den manglende forklarlighed – og dermed skjulte risiko for diskrimination – som er beskrevet ovenfor, kan i yderste konsekvens få negativ indflydelse på **retten til effektive retsmidler**.[30] Denne ret indebærer, at individet skal kunne efterprøve enhver foranstaltning, som har indflydelse på vedkommendes øvrige rettigheder.

Endelig kan overvågning i sidste ende påvirke **menneskets værdighed**, som er anerkendt i bl.a. EU's Charter.[31] Påvirkning af retten til værdighed kan f.eks. følge af, at omfattende overvågning kan blive adfærdsændrende i en sådan grad, at menneskets mulighed for at leve et værdigt liv bringes i fare.

Ovenstående viser, at de forskellige rettigheder er forbundne, og retten til privatliv og beskyttelse af personoplysninger ikke kan ses isoleret. Etablering af et privat rum for individet er en forudsætning for både personlig udvikling og aktiv deltagelse i demokratiet.[32]

---

[27] EU's Charter artikel 11 og EMRK artikel 10 (ytringsfrihed) og EU's Charter artikel 12 og EMRK artikel 11 (forsamlingsfrihed).
[28] Se også European Union Agency for Fundamental Rights, Facial recognition technology: Fundamental rights considerations in the context of law enforcement, April 2019, pkt. 7.4 og CAHAI, Feasibility Study, 17. december 2020, afsnit 3.3.1, pkt. 26.
[29] EU's Charter artikel 21, EMRK artikel 14 og artikel 12 i protokol nr. 12 til EMRK.
[30] EU-Chartrets artikel 47 og EMRK artikel 13.
[31] Artikel 1 i EU's Charter om Grundlæggende Rettigheder.
[32] CAHAI, Feasibility Study, 17. december 2020, afsnit 3.3.1. pkt. 25.

3.2.3 Praksis fra EU-domstolen

Det er de nationale domstole og i sidste ende EU-domstolen og Den Europæiske Menneskerettighedsdomstol, der afgør, om et indgreb er i strid med henholdsvis EU´s Charter og EMRK.

Forbud mod generel og udifferentieret indsamling og anvendelse af data (logning)

EU-domstolen har i flere sammenhænge taget stilling til foreneligheden med EU's charter i forhold til regler, der påbyder generel og udifferentieret registrering og anvendelse af bl.a. trafik- og lokaliseringsdata vedrørende alle borgere uafhængigt af, om der er en mistanke om strafbart forhold mod de pågældende. Disse afgørelser er på flere måder centrale for forståelsen af, hvor langt myndigheder kan gå i forhold til indgreb i retten til privatliv og beskyttelse af personoplysninger gennem bredspektret overvågning af borgernes data. Dommene er således et væsentlig bidrag til at klarlægge og forstå, hvilke begrænsninger, som proportionalitetsprincippet og princippet om formålsbegrænsning i praksis udgør for myndighedernes muligheder for at iværksætte masseregistrering eller masseovervågning.

Allerede siden Digital Rights-dommen fra 2014 [33], hvor EU-domstolen fandt, at EU's logningsdirektiv[34] var i strid med EU-retten og charterets artikler 7, 8 og 52, stk. 1, har det stået klart, at selv et utvivlsomt legitimt formål som bekæmpelse af grov kriminalitet ikke kan bære et indgreb, hvor så godt som alle borgere får deres tele- og internetdata registreret, fordi det ikke kan anses for 'strengt nødvendigt'.[35] Domstolen bemærkede bl.a., at logningsdirektivet havde "... *overskredet de grænser, som overholdelse af proportionalitetsprincippet kræver...*" gennem den særdeles bredspektrede registrering og opbevaring (logning) af teledata, som direktivet vedrørte. Domstolen bemærkede i den forbindelse, at den brede og udifferentierede registrering "... *indebærer ... et indgreb i de grundlæggende* rettigheder *for praktisk talt hele den europæiske befolkning*". [36]

Dette er også efterfølgende blevet slået fast af EU-domstolen i flere afgørelser vedrørende forskellige landes nationale logningsregler. I Tele2-dommen fra 2016 [37] udtalte domstolen, at en national lovgivning, der navnlig ikke er begrænset til en lagring, som er rettet mod data vedrørende et tidsrum og/eller et geografisk område og/eller en personkreds, derved overskrider det strengt nødvendige

[33] EU-domstolens afgørelse af 8. april 2014 (Forenede sager C-239/12 og C-594/12).
[34] Europa-Parlamentet og Rådet direktiv 2006/24/EF, som havde til formål at harmonisere medlemsstaternes bestemmelser om teleudbyderes pligtmæssige generelle og udifferentierede registrering og opbevaring ('logning') af teledata med henblik på at sikre, at der er adgang til teledata i forbindelse med efterforskning, afsløring og retsforfølgning af grov kriminalitet.
[35] Langsted og Jakobsen (2014) og Justitias analyse af 5. september 2014 om de danske logningsreglers forenelighed med de grundlæggende rettigheder.
[36] Tilsvarende i EU-domstolens afgørelse af 8. april 2014 (Forenede sager C-239/12 og C-594/12), præmis 27. Se om dommens betydning for danske regler om de danske logningsreglers forenelighed med de grundlæggende rettigheder Justitias rapport fra 4. september 2014 om hvorvidt de danske logningsregler om teleselskabers pligt til i retsplejelovens § 786, stk. 4, at foretage generel og udifferentieret logning af teledata er i strid med EU's charter samt besvarelse af spørgsmål nr. 1578 fra Folketingets Retsudvalg. Se også Langsted og Jakobsen (2009) om dommens præmisser 56-59.
[37] EUD af 21. december 2016 (forenede sager C-203/15 og C-C-698/15).

og ikke kan anses for at være begrundet i et demokratisk samfund, således som det er påkrævet i henhold til bl.a. EU-chartrets artikel 7 (ret til respekt for privatliv og familieliv), artikel 8 (ret til beskyttelse af personoplysninger) og artikel 11 (ret til ytrings- og informationsfrihed).[38] I La Quadrature-dommen fra 2020 er det om hensynet til beskyttelse af retten til privatliv anført, at oplysningerne tilsammen er egnede til at "*afsløre oplysninger om en lang række forhold, der vedrører de berørte personers privatliv (...)* og vil "*kunne gøre det muligt at drage meget præcise slutninger vedrørende privatlivet for de personer, hvis data er blevet lagret, såsom vaner i dagligdagen, midlertidige eller varige opholdssteder, daglige eller andre rejser, hvilke aktiviteter der udøves, disse personers sociale relationer og de sociale miljøer, de frekventerer. Særligt gør disse data det muligt at lave en profil af de berørte personer, hvilken oplysning, henset til retten for respekt af privatlivet, er lige så følsom som selve indholdet af kommunikationen".* [39]

Andre afgørelser om betingelser for overvågning

EU-domstolens domme om overvågning af elektronisk kommunikation vedrører en helt særligt omfattende form for overvågning, der samtidig indgår i en kompleks kontekst, idet indsamlingen sker i den private sektor og de modstående hensyn er terrorbekæmpelse og efterforskning af alvorlig kriminalitet. I relation til myndigheders mere afgrænsede overvågning, som f.eks. videoovervågning, har domstolen fastslået, at et grundlæggende element i vurderingen af indgrebets intensitet er, om der er tale om et begrænset datasæt, og om det ud fra data er muligt at tegne en profil eller fastslå bevægelsesmønstre.[40]

I relation til retsgrundlagets indhold har Menneskerettighedsdomstolen flere gange fastslået, at der gælder et krav om lovkvalitet, dvs. at retsgrundlaget skal være tilgængeligt, forudsigeligt og i overensstemmelse med 'the rule of law'.[41] Det skal være muligt at forudse sin retsstilling (hensynet til gennemsigtighed og *foreseeability*).[42] Kravet om forudsigelighed udelukker ikke, at myndigheder overlades et skøn. Det er dog forudsat, at omfanget af skønnet og den måde, hvorpå det skal udøves, er angivet med tilstrækkelig klarhed, når der tages hensyn til de anerkendelsesværdige formål, der forfølges, og at individet ydes passende beskyttelse mod vilkårlige indgreb fra det offentlige.[43] Behovet for klarhed i hjemmelsgrundlaget begrundes af domstolen bl.a. i udviklingen af den teknologi, der bruges til at udføre indgreb i privatlivet.[44] Ved særligt indgribende og hemmelig overvågning bør retsgrundlaget i det mindste omfatte en definition af de kategorier af mennesker, der kan være genstand for overvågning, en begrænsning af foranstaltningens varighed, proceduren

[38] Se også bemærkninger til lovforslag L191 af 26. april 2017 med revision af danske logningsregler som følge af Tele2-dommen om præmis 106 og 107.
[39] EUD af 6. oktober 2020 (forenede sager C-511/18, C-512/18 og C-520/18), se præmis 117.
[40] EUD af 30. januar 2020, Case of Breyer (C-82/14), præmis 92.
[41] Den Europæiske Menneskerettighedskonvention med kommentarer af Peer Lorenzen m.fl., art. 1-9, 3. udg.
[42] Se f.eks. EMD af 4. maj 2000, Rotaru vs. Rumænien, præmis 50- 52.
[43] Den Europæiske Menneskerettighedskonvention med kommentarer af Peer Lorenzen m.fl., art. 1-9, 3. udg.
[44] Se f.eks. EMD af Uzun v. Germany (4378/02) præmis 61.

for undersøgelse, anvendelse og lagring af de indsamlede data samt forholdsregler for videregivelse af data til andre parter.[45]

I en konkret sag om privat *videoovervågning* i Rumænien har EU-domstolen bl.a. slået fast, at den legitime interesse, der ligger til grund for et overvågningstiltag, som griber ind i retten til beskyttelse af privatliv og personoplysninger, skal være eksisterende og effektiv på tidspunktet for behandlingen og ikke have en hypotetisk karakter[46]. I den konkrete sag fandt domstolen, at dette var tilfældet, da der – trods andre sikkerhedsforanstaltninger – rent faktisk var sket kriminalitet af den art, som overvågningen tog sigte på at bekæmpe. Det blev dog ikke anset for at være et ufravigeligt krav, at sådan kriminalitet var foregået, for at overvågningen kunne anses for legitim.[47]

Derudover slog domstolen fast, at undtagelser fra beskyttelsen af personoplysninger skal holdes indenfor det *strengt nødvendige,* og at dette indebærer, at der i afvejningen mellem hensynet til den registreredes beskyttelse og den legitime interesse, der ønskes forfulgt, skal indgå, om dette hensyn kan tilgodeses ved andre, mindre indgribende midler.[48] Denne betingelse skulle endvidere undersøges i sammenhæng med princippet om *dataminering*, som indebærer, at behandling af personoplysninger skal være relevant og tilstrækkelig og ikke omfatte mere end, hvad der kræves i forhold til det formål, de er indsamlet til og senere vil blive anvendt til. Domstolen gav her som eksempel, at det f.eks. kunne være relevant at undersøge, om det var tilstrækkeligt, at videoovervågningen kun er aktiv om natten eller udenfor normal arbejdstid, og blokere eller sløre billeder, som optages på steder, hvor overvågningen ikke er nødvendig.[49]

3.2.4 Det Europæiske Databeskyttelsesråd (EDPB)

Det Europæiske Databeskyttelsesråd (EDPB)[50] har udarbejdet en række retningslinjer og anbefalinger af betydning for overvågningsområdet, som i vidt omfang baserer sig på EU-domstolens praksis. I Databeskyttelsesrådets retningslinjer om brug af videoudstyr til behandling af personoplysninger har EDPB udlagt EU-domstolens praksis på den måde, at videoovervågning kun bør vælges, hvis formålet med behandlingen ikke med rimelighed kan opfyldes på anden måde, som er mindre indgribende i den registreredes grundlæggende rettigheder og frihedsrettigheder.[51] Derudover har EDPB tilkendegivet, at registrerede med rimelighed bør kunne forvente at være fri for overvågning på offentlige områder, navnlig på områder, der typisk anvendes til rekreative formål og fritidsaktiviteter

[45] EMD af 29 June 2006, Weber and Saravia (54934/00), præmis 92-95.
[46] EUD af 11. december 2019, Case of TK (C-708/18), præmis 44-45.
[47] EUD af 11. december 2019, Case of TK (C-708/18), præmis 44.
[48] EUD af 11. december 2019, Case of TK (C-708/18), præmis 46-47.
[49] EUD af 11. december 2019, Case of TK (C-708/18), præmis 51. Se også EDPB Retningslinjer 3/2019 af 29. januar 2020 om brug af videoudstyr til behandling af personoplysninger, afs. 3, pkt. 15.
[50] European Data Protection Board (EDPB).
[51] EDPB Retningslinjer 3/2019 af 29. januar 2020 om brug af videoudstyr til behandling af personoplysninger, afs. 3, pkt. 24

(...), idet den registreredes interesser eller rettigheder og frihedsrettigheder her ofte vil gå forud for øvrige legitime interesser[52].

Endvidere har EDPB har på baggrund af en analyse af de væsentligste domme fra EU-domstolen om tredjelandsoverførsler[53] formuleret *en række principper eller væsentlige garantier*, der vedrører de retlige krav, som i henhold til det Europæiske Charter for grundlæggende rettigheder må anses som centrale i forhold til at vurdere andre landes lovgivningsmæssige beskyttelsesniveau i forhold til beskyttelse mod indgreb i retten til databeskyttelse og privatlivets fred. [54]

A. Behandling skal være baseret på klare, præcise og tilgængelige regler.

B. Nødvendighed og proportionalitet, hvad angår de legitime mål, der forfølges, skal godtgøres.

C. Der skal findes en uafhængig tilsynsmekanisme.

D. Der skal være effektive retsmidler til rådighed for de enkelte personer.

Principperne er baseret på de grundlæggende rettigheder til privatlivets fred og databeskyttelse, der gælder for alle uanset nationalitet. Selvom principperne er fremkommet i en anden kontekst, er de også anvendelige som klarlæggelse af de fundamentale krav, som følger af EU's charter – og som således skal indtænkes i forbindelse med overvågning.[55]

3.3 Delkonklusion

Den menneskeretlige beskyttelse af retten til privatliv og beskyttelse af personoplysninger indebærer, at staten kun kan gøre indgreb i disse rettigheder, hvis der foreligger et legitimt formål, et klart retsgrundlag og indgrebet findes nødvendigt og proportionalt i et demokratisk samfund. Staten har samtidig pligt til at sikre, at behandlingen af borgernes oplysninger sker til udtrykkeligt angivne saglige formål, på en rimelig og gennemsigtig måde, jf. herved den særlige beskyttelse af behandling af personoplysninger i EU's Charters artikel 8.

Indgreb i borgernes ret til privatliv i form af myndighedsmæssig overvågning af fysiske borgere vil typisk udgøre behandling af personoplysninger. Det indebærer, *at* indsamling og brug af oplysningerne skal kunne anses for at forfølge et **legitimt formål,** *at* overvågningen skal være aktuel og effektiv og ikke have hypotetisk karakter i forhold til at opnå det påtænkte resultat.[56] Derudover skal overvågningen være baseret på et **klart retsgrundlag**, som indebærer krav til retsgrundlagets kvalitet og præcision i forhold til, hvem der er omfattet, og hvilke formål overvågningen tjener.

[52] EDPB Retningslinjer 3/2019 om brug af videoudstyr til behandling af personoplysninger, version 2.0. af 29. januar 2020, afsnit 3.1.3.2, punkt 36.
[53] Analyse af bl.a. EUD af 6. oktober 2015 (Schrems I - C-362/14) og EUD af 16. juli 2020 (Schrems II - sag C-311/18), EUD om La Quadrature du Net (forenede sager C-511/18, C-512/18 og C-520/18), EUD om Privacy International (C.-623/17).
[54] EDPB - Anbefalinger 02/2020 om de europæiske væsentlige garantier for overvågningsforanstaltninger. Vedtaget den 10. november 2020, afsnit 3, punkt 24.
[55] EDPB - Anbefalinger 02/2020 om de europæiske væsentlige garantier for overvågningsforanstaltninger. Vedtaget den 10. november 2020, afsnit 3.
[56] EUD af 11. december 2019, Case of TK (C-708/18), præmis 46-47 (privat videoovervågning).

Navnlig når der er tale om et intensivt indgreb, skal retsgrundlaget være specifikt i relation til, hvem og hvad der er omfattet af overvågningen, samt indeholde en begrænsning af foranstaltningens varighed, proceduren for undersøgelse, anvendelse og lagring af de indsamlede data samt forholdsregler for videregivelse af data til andre parter.[57] Derudover er det et krav, at indgrebet ikke går videre end det, som er **nødvendigt** og **proportionelt** i et demokratisk samfund. Overvågningen skal derfor være nødvendig og forholdsmæssig i forhold til det påtænkte formål, dvs. overvågningen skal udgøre det mindst mulige indgreb, der er egnet til at opnår formålet, herunder i tid og sted. Der bør således ske en meget nøje afvejning af overvågning i tid og sted, hvor det har betydning, hvor intensivt et indgreb der er tale om, herunder hvor mange mennesker det berører og hvilke dele af privatlivet der påvirkes. Det vil også have betydning, hvor tungtvejende samfundsmæssige formål, der forfølges og samt om det er muligt at begrænse indgrebet.[58]

Hvis der er tale om mange oplysninger, og det ud fra de indsamlede data er muligt at tegne en profil eller fastslå bevægelsesmønstre for mange borgere, må indgrebet anses for at være særligt indgribende. Statens forpligtelser efter EU´s charters artikel 8 må ved sådanne indgreb i særlig grad anses at indebære kvalificerede krav til, at oplysningerne behandles på en **rimelig** måde og til **udtrykkeligt angivne formål,** hvilket samlet må anses at indebære en særlig forpligtelse til at sikre **gennemsigtighed**.

[58] Se bla. EMD af 4. maj 2000, Rotaru vs. Rumænien, præmis 50- 52.

4 De databeskyttelsesretlige regler

Der findes ikke en egentlig overvågningsret. Uden for efterretningsområdet bliver databeskyttelsesretten derfor retssystemets hovedregulering af overvågning, fordi personovervågning typisk indebærer behandling af personoplysninger i form af billeder med genkendelige ansigter eller andre personhenførbare data.[59]

Da digitaliseringen samtidig har øget omfanget af strukturerede personoplysninger, som ved hjælp af it og teknologiske analyseværktøjer kan gøres til genstand for overvågning, er regler om persondatabeskyttelse blevet af afgørende betydning for at kunne sikre beskyttelsen af borgernes privatliv.

I afsnit 5.1 nedenfor gennemgås det databeskyttelsesretlige regelgrundlag, mens afsnit 5.2 behandler de databeskyttelsesretlige grundprincipper i databeskyttelsesforordningens artikel 5. I afsnit 5.2 sættes særlig fokus på datasamkøring i kontroløjemed. Kapitlet afsluttes med en delkonklusion i afsnit 5.4.

4.1 EU-regler og nationale regler

Danmark har altid været førende inden for regulering af elektronisk behandling af borgernes oplysninger. Med registerlovene, som trådte i kraft i 1979 på baggrund af udvalgsarbejde startet op tilbage i 1973, var Danmark blandt de allerførste lande, der regulerede både privates og offentlige myndigheders registre og behandling af personoplysninger. Lov om offentlige myndigheders registre fra 1979 havde til formål at sikre, at offentlige myndigheders oprettelse og brug af registre med personoplysninger, hvortil der anvendes elektronisk databehandling, skete på en sådan måde, at den enkelte borgers retsbeskyttelse ikke blev krænket.[60]

I 2000 afløstes de hidtil gældende registerlove af persondataloven,[61] som bl.a. udmøntede EU's direktiv[62] på området. Persondataloven var – med mindre ændringer – gældende frem til 2018, hvor loven den 25. maj 2018 blev afløst af **EU's databeskyttelsesforordning (GDPR)** og den **supplerende nationale databeskyttelseslov**.[63] Disse to regelsæt udgør nu den grundlæggende regulering af rammerne for behandling af personoplysninger i Danmark.

Databeskyttelsesforordningen gælder imidlertid ikke for retshåndhævende myndigheders behandlinger af personoplysninger med henblik på at forebygge, efterforske, afsløre eller

[59] Blume (2014): Overvågning. Kan persondataretten gøre nytte? S. 69.
[60] Betænkning om behandling af personoplysninger, nr. 1345/1997, afsnit 2.1.
[61] Lov nr. 429 af 31. maj 2000 om behandling af personoplysninger.
[62] Europa-Parlamentets og Rådets direktiv 95/46 EF af 24. oktober 1995 om beskyttelse af fysiske personer i forbindelse med behandlinger af personoplysninger mv.
[63] Europa-Parlamentets og Rådets forordning 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandlinger af personoplysninger mv. (GDPR) og lov nr. 502 af den 23. maj 2018 om supplerende bestemmelser til forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (databeskyttelsesloven).

retsforfølge strafbare handlinger eller fuldbyrde strafferetlige sanktioner, herunder beskytte mod og forebygge trusler mod den offentlige sikkerhed.[64] De retshåndhævende myndigheder er navnlig bl.a. politiet, anklagemyndigheden og kriminalforsorgen. For disse myndigheders behandling af personoplysninger – med retshåndhævende formål - gælder **EU's retshåndhævelsesdirektiv,**[65] som er gennemført i dansk ret ved **retshåndhævelsesloven**[66] De retshåndhævende myndigheder må i henhold til denne lov behandle oplysninger, når behandling er *nødvendig* for at forebygge, efterforske, afsløre eller retsforfølge strafbare handlinger eller fuldbyrde strafferetlige sanktioner, herunder for at beskytte mod eller forebygge trusler mod den offentlige sikkerhed.[67] Direktivet og loven indeholder en række grundlæggende behandlingsprincipper,[68] som i hovedsagen svarer til de principper, der følger af databeskyttelsesforordningens artikel 5, om end reglerne er tilpasset retshåndhævelsesområdet.

4.2 De databeskyttelsesretlige grundprincipper i artikel 5

Databeskyttelsesrettens "grundlov" eller grundlæggende principper er fastlagt i databeskyttelsesforordningens artikel 5, som i overensstemmelse med artikel 8 i EU's charter helt overordnet påbyder, at *personoplysninger skal behandles på en lovlig, rimelig og gennemsigtig måde.*[69] Bestemmelsen svarer i det store hele den tidligere persondatalovs § 5, og principperne har med andre ord været gældende i Danmark siden 2000.[70]

Databeskyttelsesforordningens artikel 5 udfolder, hvad der nærmere ligger i at behandle personoplysninger lovligt, rimeligt og gennemsigtigt med det overordnede formål at beskytte individers rettigheder og friheder i forbindelse med behandling af personoplysninger. Behandlingsbegrebet er meget bredt og omfatter bl.a. indsamling, registrering, systematisering, genfinding, videregivelse, sammenstilling eller samkøring af data.[71]

Databeskyttelsesretten spiller sammen med hele retssystemet Er en fremgangsmåde ikke i overensstemmelse med et eller flere af de databeskyttelsesretlige principper, kan det betyde, at en ellers lovhjemlet behandling ikke kan finde sted. På den måde fungerer artikel 5 som en slags generalklausul.[72]

---

[64] Databeskyttelsesforordningens artikel 2, stk. 2, litra d, samt Kommentar til databeskyttelsesforordningen (2020) s. 221f.
[65] Europa-Parlamentets og Rådets direktiv (EU) 2016/680 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med kompetente myndigheders behandling af personoplysninger med henblik på at forebygge, efterforske, afsløre eller retsforfølge strafbare handlinger eller fuldbyrde strafferetlige sanktioner og om fri udveksling af sådanne oplysninger mv.
[66] Lov nr. 410 af 27. april 2017 om retshåndhævende myndigheders behandling af personoplysninger, som regulerer politiets behandlinger af personoplysninger med henblik på at forebygge, efterforske, afsløre eller retsforfølge strafbare handlinger mv.
[67] Retshåndhævelseslovens § 9.
[68] Retshåndhævelseslovens § 4.
[69] Artikel 5, stk. 1, litra a.
[70] Lov nr. 429 af 31. maj 2000 om behandling af personoplysninger.
[71] Databeskyttelsesforordningens art. 4, nr. 2 med eksempler på behandlinger.
[72] Blume (2014) Overvågning. Kan persondataretten gøre nytte?

Udover de helt overordnede principper om lovlighed, rimelighed og gennemsigtighed, fastsætter bestemmelsen princippet om *formålsbegrænsning.*[73] Princippet indebærer, at oplysninger skal indsamles til udtrykkeligt angivne og legitime formål og ikke må viderebehandles på en måde, der er uforenelig med disse formål. Derudover indeholder bestemmelsen principperne om *dataminimering og rigtighed*. Disse principper indebærer pligt til kun at behandle korrekte personoplysninger og kun i det omfang, det er tilstrækkeligt, relevant og nødvendigt og dermed *proportionelt* i forhold til behandlingsformålet.[74] Der gælder også krav til *opbevaringsbegrænsning,* som betyder, at personoplysninger ikke må opbevares på en måde, hvor de pågældende kan identificeres i længere tid end det som er nødvendigt i forhold til behandlingsformålet.[75] Endelig stilles der krav til *persondatasikkerheden*, som indebærer en pligt til at sikre opbevaring og håndtering, så personoplysninger ikke udsættes for misbrug, tab, ødelæggelse eller beskadigelse.[76]

Princippet om sikkerhed bliver tiltagende vigtig i takt med digitaliseringen af myndighedernes behandling af stadig større mængder af personoplysninger. Dette skyldes, at dataindsamling, registrering og opbevaring af oplysninger i sig selv skaber en risiko for, at der på et senere tidspunkt kan ske persondatamisbrug.[77] Det falder udenfor rapportens fokus at gå mere i dybden med de retssikkerhedsmæssige problemstillinger, der knytter sig til manglende persondatasikkerhed, men det fremhæves dog, at der årligt rapporteres mellem 8.000–9.000 brud på persondatasikkerheden i Danmark. Mere end halvdelen vedrører offentlige myndigheder og mange vedrører brud på fortroligheden eller tab af oplysninger i systemer med mange borgeres oplysninger.[78]

Visse af de grundlæggende principper må anses for at være helt afgørende, når behandling sker som led i overvågning, og disse vil blive behandlet lidt nærmere i det følgende. Det drejer sig om **proportionalitetsprincippet**, som indebærer, at der kun må behandles personoplysninger i nødvendigt omfang. [79] Dette er nærmere behandlet i afsnit 4.2.1. Det andet er **princippet om formålsbegrænsning**, som indebærer, at personoplysninger kun må indsamles til udtrykkeligt angivne og legitime formål og som udgangspunkt ikke efterfølgende må viderebehandles på en måde, der er *uforenelig* med disse formål. Dette er nærmere behandlet i afsnit 4.2.2. **Princippet om rigtighed** får særligt relevans, når indsamlede personoplysninger tages i anvendelse i en myndighedssag, og er nærmere behandlet i afsnit 4.2.3. Endelig berøres i afsnit 4.2.4 **princippet om ansvarlighed** i tilknytning til gældende processuelle krav og garantiforskrifter, som er særligt relevante ved iværksættelse af nye indgribende behandlinger af personoplysninger, hvilket overvågning typisk vil udgøre.

[73] Artikel 5, stk.1, litra b.
[74] Artikel 5, stk.1, litra c og litra d.
[75] Artikel 5, stk.1, litra e.
[76] Artikel 5, stk.1, litra f.
[77] Blume (2014) Overvågning. Kan persondataretten gøre nytte?
[78] Udviklingen i antal og typer af sikkerhedsbrud kan følges på Datatilsynets hjemmeside: Statistik over brud på persondatasikkerheden.
[79] Blume (2014) Overvågning. Kan persondataretten gøre nytte?

4.2.1 Proportionalitetsprincippet i forhold til overvågning

Navnlig principperne om dataminimering, opbevaringsbegrænsning og nødvendighed er udtryk for en generelt gældende grundsætning om proportionalitet, som indebærer, at der kun må indsamles, opbevares og videregives oplysninger om den enkelte person som led i overvågning i det omfang, det er nødvendigt i forhold til overvågningens formål. Proportionalitetskravet vedrører ikke kun antallet af oplysninger eller deres relevans for overvågningsformålet. Princippet forsætter også en vurdering af de pågældende oplysningers *egnethed* til at realisere formålet med den iværksatte overvågning. På et generelt plan skal den dataansvarlige derfor foretage en kvalitativ bedømmelse af de oplysninger, der vil blive indsamlet. Det er i forhold til *massen*, at overvågningens proportionalitet skal vurderes, og der må ikke må indsamles eller opbevares flere oplysninger end det, der er nødvendigt for at opfylde overvågningens formål. [80]

EU-domstolens afgørelser (se afsnit 4.2.3) om lovligheden af regler om generel og udifferentieret registrering og opbevaring af trafik- og lokalitetsdata vedrørende alle borgeres telekommunikation har særlig relevans i forhold til vurderingen af, hvorvidt et overvågningstiltag er proportionelt og dermed foreneligt med de grundlæggende principper.[81]

4.2.2 Princippet om formålsbegrænsning i forhold til overvågning

Princippet om formålsbegrænsning indebærer i praksis ikke et absolut forbud mod at behandle oplysninger til nye formål, som er uforenelige med det eller de formål, som oplysningerne er indsamlet til. Forordningen åbner nemlig op for et *nationalt råderum*, som giver medlemsstaterne mulighed for at fastsætte regler, der fraviger forordningens krav til bl.a. formålsbegrænsning og oplysningspligt. [82] Fravigelse forudsætter dog, at tiltaget findes at være en nødvendig og forholdsmæssig foranstaltning i et demokratisk samfund og forfølger et legitimt formål i relation til bl.a. generelle samfundsmæssige interesser som væsentlige økonomiske finansielle interesser, folkesundhed, social sikkerhed eller til kontrol-, tilsyns- eller reguleringsfaktorer.

Det er imidlertid fortsat en betingelse, at sådan begrænsning *respekterer det væsentligste indhold af de grundlæggende rettigheder og frihedsrettigheder*. Derudover skal enhver fravigelse som minimum indeholde specifikke bestemmelser om bl.a. formålene med behandlingen, rækkevidden af de indførte begrænsninger, opbevaringsperioder og gældende garantier under hensyntagen til behandlingens karakter, omfang og formål eller kategorier af behandling samt risiciene for de registreredes rettigheder, dvs. krav der sigter mod fortsat at sikre lovlighed, rimelighed og gennemsigtig i behandlingen af oplysninger.[83] Af forordningens indledende bemærkninger fremgår det endvidere, at der i forbindelse med sådan fravigelse navnlig skal være opmærksomhed på at

[80] Blume (2014) Overvågning. Kan persondataretten gøre nytte? S. 71.
[81] Langsted og Jakobsen (2014): I en højere sags tjeneste. Afvejningen mellem overvågning og privatliv i en retlig kontekst.
[82] Databeskyttelsesforordningens præambelbetragtning nr. 10 samt i forhold til de registreredes rettigheder artikel 23.
[83] Databeskyttelsesforordningen med kommentarer, 1. udgave (2020) side 583ff

sikre borgernes rettigheder i forhold til at få information om de andre formål og om deres ret til at gøre indsigelse.[84]

4.2.3 Princippet om rigtighed

Det er helt grundlæggende for al myndighedsudøvelse, at den foretages på et korrekt grundlag, hvilket også er afspejlet i det databeskyttelsesretlige grundprincip om rigtighed i artikel 5, stk.1 litra d. Det følger heraf, at oplysninger skal være korrekte og om nødvendigt ajourførte, ligesom der er pligt til at tage *ethvert rimeligt skridt* for at sikre, at der ikke behandles urigtige oplysninger i forhold til den sammenhæng, hvori de indgår.[85] Kravet indebærer imidlertid ikke en pligt til straks at ajourføre og kontrollere alle personoplysninger, der indsamles og behandles.[86] Særligt i forhold til overvågning vil princippet dog kunne få betydning, når indsamlede personoplysninger tages i anvendelse i en myndighedssag og indgår i dataovervågning som led i datasamkøring og lignende. Det kan f.eks. være i de tilfælde, hvor der rejses kontrolsager på baggrund af resultaterne af en datasamkøring, eller hvor oplysninger genanvendes og sammenstilles som led i en profilering af borgere og anvendes beslutningsunderstøttende. I sådanne situationer vil det være relevant at have et skærpet fokus på, om de oplysninger, der er indsamlet til ét formål, også er korrekte og tilstrækkeligt ajourførte i forhold til de nye formål, de ønskes anvendt til.

4.2.4 Princippet om ansvarlighed og krav om konsekvensanalyser

Princippet om ansvarlighed (accountability) er dels fastsat i artikel 5, stk. 2, og dels i artikel 24. Artikel 5, stk. 2, indebærer grundlæggende, at den, der behandler oplysninger, skal kunne *påvise*, at de grundlæggende principper er overholdt. Princippet om ansvarlighed er gennemgående i mange af forordningens bestemmelser, og er udtryk for, at den, der har interesse i at indsamle og bruge personoplysningerne, også står inde for og aktivt har pligt til at sikre sig, at de behandles *på en lovlig, rimelig og gennemsigtig måde*.[87] Artikel 24, stk. 1, fastslår eksempelvis, at den dataansvarlige både før en behandling startes op og løbende derefter skal gennemføre passende tekniske og organisatoriske foranstaltninger for at sikre og for at være i stand til at påvise, at behandling er i overensstemmelse databeskyttelsesforordningens regler.

Ansvarlighedsprincippet er bl.a. afspejlet i krav om ***risikovurdering***, henholdsvis udarbejdelse af ***konsekvensanalyse***, når der er tale om særligt indgribende behandlingsformer, som med forordningens ord *sandsynligvis vil indebære en høj risiko for fysiske personers rettigheder og frihedsrettigheder*.[88] En konsekvensanalyse indebærer en vurdering af de påtænkte behandlingsaktiviteters konsekvenser for beskyttelsen af personoplysninger og har til formål at sikre

[84] Se præambelbetragtning nr. 50
[85] Artikel 5, stk.1, litra d.
[86] Databeskyttelsesforordningen med kommentarer, 1. udgave (2020), s. 332, hvor det dog er anført, at pligten til ajourføring formentlig må anses for skærpet i kraft af forordningen i forhold til det som tidligere fulgte af persondataloven.
[87] Databeskyttelsesforordningen med kommentarer, 1. udgave (2020) s. 341 og s. 689.
[88] Databeskyttelsesforordningens artikel 35 og præambelbetragtninger 84, 89 ff.

en særlig opmærksomhed på borgernes rettigheder *inden* iværksættelse af indgribende databehandlinger.[89] Konsekvensanalyser er særligt relevante at gennemføre, når der behandles meget store mængder oplysninger, anvendes ny teknologi og behandles biometriske data.[90] Overvågningsmæssige aktiviteter er direkte nævnt i forordningens bestemmelse om konsekvensanalyser både i relation til systematisk og omfattende vurdering af personlige forhold vedrørende fysiske personer, der er baseret på automatisk behandling, herunder profilering,[91] samt i relation til systematisk overvågning af et offentligt tilgængeligt område i stort omfang.[92]

Også *retshåndhævelsesloven* stiller krav om udarbejdelse af konsekvensanalyser,[93] og selvom de ikke er formuleret lige så eksplicit, er kriterierne og beskyttelseshensynet det samme. Bestemmelserne er udformet i overensstemmelse med retshåndhævelsesdirektivets regler, som i det store hele svarer til databeskyttelsesforordningens regler.[94]

4.3 Datasamkøring i kontroløjemed (systematisk dataovervågning)

Videregivelse af personoplysninger mellem myndigheder med henblik på samkøring i kontroløjemed er et område, der allerede før den EU-retlige lovgivning på området har haft et særligt fokus i Danmark. Grundlæggende er samkøring af personoplysninger en fremgangsmåde, der indebærer, at staten ved at kombinere forskellige informationer får en større viden om sine borgere. Dette kan i nogle – men langt fra alle – tilfælde føre til, at der opstilles en profil over den enkelte borger og dennes relation til de offentlige myndigheder.[95] Hvis samkøring sker i *kontroløjemed,* kan en sådan behandling typisk blive indgribende for et større antal borgere. Derfor er samkøring i kontroløjemed altid blevet anset for en mere indgribende form for behandling, der stiller særlige krav til bl.a. lovlighed, proportionalitet og gennemsigtighed.[96]

En meget væsentlig årsag til indførelsen af den oprindelige registerlovgivning i 1979 var netop *frygten for registersamkøringer*. Indførelsen af personnummeret i 1968 havde nemlig ført til, at alle danskere med stor sikkerhed ville kunne identificeres entydigt på tværs af offentlige registre og databaser. Samkøring eller sammenstilling af oplysninger om bestemte personer fra flere registre eller databaser blev opfattet som det mest tydelige eksempel på, at Danmark som en følge af informationsteknologien risikerede at blive et Big Brother-samfund.[97]

Folketingets Retsudvalg forudsatte derfor helt tilbage i 1991 i forbindelse med en ændring af de dagældende registerlove, at myndighederne i forbindelse med samkøring i kontroløjemed skal have

[89] Databeskyttelsesforordningen med kommentarer, 1. udgave (2020) s. 689 og præambelbetragtning 84.
[90] Præambelbetragtninger nr. 89-91.
[91] Databeskyttelsesforordningens artikel 35, stk.3, litra a.
[92] Databeskyttelsesforordningens artikel 35, stk.3, litra c.
[93] Retshåndhævelseslovens §§ 25-26.
[94] Lovforslag L168 af 28. marts 2017, alm. Bemærkninger, afsnit 2.5.3.5 samt artikel 27 og 28 i retshåndhævelsesdirektivet.
[95] Blume og Herrmann (2018) s. 312.
[96] Databeskyttelsesforordningen og databeskyttelsesloven med kommentarer af Nielsen, K.K. & Lotterup, A., 1. udgave (2020), afsnit 2.5.2, s. 379.
[97] Blume og Herrmann (2018) s. 313.

et *klart og utvetydigt retsgrundlag*, og at myndighederne kun må lade kontrolordningen tage sigte på fremtidige forhold, medmindre særlige forhold gør sig gældende. Flertallet lagde endvidere vægt på, at de borgere, som berøres af kontrolordningen, i almindelighed skal gøres opmærksom på myndighedernes adgang til at foretage samkøringen i kontroløjemed, inden kontrollen iværksættes, og at samkøring om muligt kun finder sted, hvis de personer, der omfattes af kontrollen, har fået meddelelse om kontrolordningen, *inden* de afgav oplysningerne til myndigheden. Endelig fandt flertallet anledning til at bemærke, at forudgående kontrol, før der træffes afgørelse, er at foretrække frem for en bagudrettet kontrol.[98] Udvalget bag betænkningen, der førte til persondataloven fra 2000, anbefalede at opretholde den restriktive retstilstand, som bl.a. indebar, at samkøring i kontroløjemed kun kunne besluttes ved lov. Udvalget bemærkede samtidigt, at samkøring af registre, der hver især er oparbejdet med henblik på varetagelse af egne særskilte formål, ville give mulighed for dannelse af meget tætte profiler af de pågældende enkeltpersoner, hvilket kunne udgøre en risiko for krænkelse af deres privatliv.[99]

Det er imidlertid ikke længere en forudsætning, at samkøring i kontroløjemed skal have særskilt lovhjemmel. Samkøring i kontroløjemed sker derfor – efter vedtagelsen af den nugældende databeskyttelseslov - baggrund af de almindelige regler i databeskyttelsesforordningen- og loven. I den juridiske litteratur er det dog fremhævet, at samkøring i kontroløjemed er en indgribende behandling, og at opmærksomheden på de almindelige databeskyttelsesretlige principper derfor skal skærpes.[100]

4.3.1 Særligt om administrativt bestemt samkøring i kontroløjemed

Det krav om direkte lovhjemmel til samkøring i kontroløjemed, som fulgte af Folketingets Retsudvalgs tilkendegivelser i 1991, var fast praksis i dansk ret frem til 2018, hvor den europæiske databeskyttelsesforordning og den supplerende danske databeskyttelseslov afløste persondataloven.

Databeskyttelsesforordningen indeholder imidlertid ikke udtrykkelige bestemmelser om myndigheders samkøring af personoplysninger i kontroløjemed. Omfattende behandlingsaktiviteter til behandling af meget store mængder oplysninger og systematisk og omfattende vurderinger af personoplysninger baseret på profilering er derimod beskrevet flere steder som en særligt indgribende form for behandling af oplysninger.[101] Profilering dækker i et vist omfang over de typer behandling, der foretages som led i samkøring i kontroløjemed.[102]

---

[98] Betænkning om behandling af personoplysninger nr. 1345/1997, afsnit 2.7.3, s. 70. Se et eksempel i Datatilsynets udtalelse af 18. juni 2006 i forbindelse med videregivelse af Udenrigsministeriets evakueringslister fra Libanon til brug for kontrol af socialt bedrageri: Anmodning om forhåndstilkendegivelse vedrørende videregivelse.
[99] Betænkning om behandling af personoplysninger nr. 1345/1997, afsnit 3.5.1.1, s. 228.
[100] Se om baggrunden herfor Databeskyttelsesforordningen og databeskyttelsesloven med kommentarer af Nielsen, K.K. & Lotterup, A., 1. udgave (2020), afsnit 2.5.2, s. 379.
[101] Se fx databeskyttelsesforordningens præambelbetragtninger 60, 71 og 91 samt artikel 35.
[102] Motzfeldt, H. M. (2018): Smarte profileringsteknologier og persondataforordningens generalklausul.

I forbindelse med implementeringen af databeskyttelsesforordningen opstod en omfattende samfundsdebat om brugen af det *nationale råderum* til vedtagelse af regler, der fraviger væsentlige databeskyttelsesretlige principper[103] og visse af borgernes databeskyttelsesretlige rettigheder. Det blev bl.a. benyttet til at lovfæste ændringer i reguleringen af myndighedsmæssig samkøring af personoplysninger.[104]

Baggrunden for den omfattende debat var, at lovforslaget til databeskyttelsesloven[105] indeholdt en bred bemyndigelsesbestemmelse i § 5, stk. 3, som gav adgang til *administrativt* – og altså ikke længere kun ved lov - at udstede regler, som fraveg det grundlæggende princip om *formålsbegrænsning* i databeskyttelsesforordningen, dvs. princippet om, at indsamlede oplysninger ikke må (gen)anvendes til formål, der er uforenelige med de formål, de er indsamlet til brug for. Der var med andre ord tale om en generel bemyndigelsesbestemmelse til, at der på administrativt niveau - udenom Folketinget - kunne fastsættes regler om samkøring i kontroløjemed, som ellers ville være i strid med det grundlæggende princip om, at oplysninger kun må anvendes til det formål, som de er indsamlet til, jf. databeskyttelsesforordningen artikel 5.[106] Det blev derudover foreslået i lovens § 23 at give mulighed for generelt at begrænse pligten til at give borgerne underretning om viderebehandling i disse tilfælde, hvorved gennemsigtigheden af databehandlingen blev svækket.

I relation til genanvendelse af oplysninger som led i samkøring i kontroløjemed udgjorde bemyndigelsesbestemmelsen en helt afgørende ændring af den hidtil gældende retstilstand. Forordningens krav om klart retsgrundlag indebærer ikke som den hidtil gældende danske praksis et krav om direkte lovhjemmel.[107] Flere høringsparter, herunder både Justitia og Institut for Menneskerettigheder, var stærkt kritiske overfor dette forslag, som på afgørende vis ville ændre rammerne for samkøring af oplysninger i kontroløjemed. Kritikken rettede sig især mod, at den demokratiske proces omkring beslutninger om yderligere samkøring i kontroløjemed risikerede at blive sat ud af spil. Derudover øgedes risikoen for uigennemsigtighed for borgerne i forhold til myndighedsmæssig anvendelse af deres oplysninger.[108]

I forbindelse med Folketingets behandling af lovforslaget til databeskyttelsesloven blev der stillet en lang række spørgsmål fra Folketingets Retsudvalg til ministeren, hvoraf størstedelen omhandlede den pågældende bemyndigelsesbestemmelse.[109] Den parlamentariske debat resulterede bl.a. i et

[103] Se ovenfor i afsnit 4.1.
[104] Lov nr. 502 af den 23. maj 2018 om supplerende bestemmelser til forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (databeskyttelsesloven).
[105] Lovforslag nr. 68 fremsat den 25. oktober 2017.
[106] Databeskyttelsesforordningens artikel 5, stk. 1, litra b.
[107] Databeskyttelsesforordningen og databeskyttelsesloven med kommentarer af Nielsen, K.K. & Lotterup, A., 1. udgave (2020), s. 161.
[108] Justitias statusrapport, december 2017, s. 5 samt høringssvar af 22. august 2017 (Institut for Menneskerettigheder), høringssvar af 17. august 2017 (IDA), høringssvar af 18. august 2017 (Rådet for Digital Sikkerhed) og høringssvar af 22. august 2017 (IT-branchen).
[109] Databeskyttelsesforordningen og databeskyttelsesloven med kommentarer af Nielsen, K.K. & Lotterup, A., 1. udgave (2020), s. 161.

ændringsforslag til lovteksten, hvorefter den generelle undtagelse fra oplysningspligt ved genanvendelse af personoplysninger som led i administrativt bestemt samkøring, *ikke* skulle finde anvendelse ved samkøring *i kontroløjemed*[110]. Desuden kom der to betænkninger fra Folketingets Retsudvalg,[111] som fastsatte en ***særlig parlamentarisk proces*** for godkendelse af bekendtgørelser udstedt i medfør af bemyndigelsesbestemmelsen.[112] Processen tog sigte på fortsat at sikre en vis demokratisk kontrol med administrative regler om bl.a. samkøring i kontroløjemed og indebar, at en minister i forbindelse med udstedelse af bekendtgørelser efter lovforslagets § 5, stk. 3, blev forpligtet til at sende et bekendtgørelsesudkast til afstemning i både Retsudvalget og det *relevante fagudvalg* i Folketinget samtidig med, at bekendtgørelsesudkastet blev sendt i høring hos Datatilsynet og andre relevante parter. Desuden forpligtede justitsministeren sig til hvert år at udarbejde årlige redegørelser til Folketinget om, hvilke bekendtgørelser der var udstedt i henhold til bemyndigelsesbestemmelsen i databeskyttelseslovens § 5, stk. 3.[113]

Intentionen med disse særlige forholdsregler var at sikre, at der fortsat ville være en vis parlamentarisk involvering og gennemsigtighed i forbindelse med beslutning om yderligere myndighedsmæssig adgang til at fravige det grundlæggende princip om formålsbegrænsning ved genanvendelse af borgernes oplysninger til nye og helt andre formål, end dem oplysningerne var indsamlet til, samt at sikre gennemsigtighed for borgerne, hvis der var tale om samkøring i kontroløjemed.[114]

Det fremgår af justitsministerens besvarelse af spørgsmål nr. 47 af 7. november 2024 (Alm. del) fra Folketingets Retsudvalg, at bemyndigelsesbestemmelsen endnu ikke har været anvendt. [115]

4.4 Delkonklusion

Databeskyttelsesforordningen indeholder en række grundlæggende principper, som i overensstemmelse med artikel 8 i EU's charter indebærer, at *personoplysninger skal behandles på en lovlig, rimelig og gennemsigtig måde.*[116] Al behandling af personoplysninger skal leve op til disse principper. Hvis det vurderes, at en fremgangsmåde ikke er i overensstemmelse med et eller flere af disse principper, kan det betyde, at en ellers lovhjemlet behandling ikke kan finde sted.

Særligt indgribende behandlingsformer som f.eks. behandling af mange oplysninger som led i videoovervågning på offentligt og frit tilgængeligt sted, systematiseret behandling af oplysninger

[110] Databeskyttelseslovens § 23, 2. punktum.
[111] Betænkninger af 9. og 16. maj 2018 til L 68 og L 69, Folketinget 2017-18.
[112] Ordningen er nærmere beskrevet her: https://www.ft.dk/samling/20181/almdel/REU/bilag/213/2030856/index.htm.
[113] Svar til Folketingets Retsudvalgs spørgsmål 102, 115 og 126 i forbindelse med behandlingen af L68, Samling 2017-18 (Databeskyttelsesloven), samt det anførte i betænkninger afgivet af Retsudvalget den 9. maj 2018, punkt 5, samt tillægsbetænkning afgivet 16. maj 2018.
[114] Betænkninger af 9. og 16. maj 2018 til L 68 og L 69, Folketinget 2017-18.
[115] Svar af 7. november 2024 til spm. 47 (alm. Del). Folketingets Retsudvalg: https://www.ft.dk/samling/20241/almdel/reu/spm/47/svar/2085428/2932222.pdf.
[116] Artikel 5, stk. 1, litra a.

som led i profilering og behandling af oplysninger ved hjælp af ny teknologi kan stille kvalificerede krav til retsgrundlagets klarhed, rimelighed og gennemsigtighed i forhold til borgeren.

Principperne er bl.a. begrundet i, at dataindsamling, registrering og opbevaring af oplysninger i sig selv skaber en risiko for, at der på et senere tidspunkt kan ske persondatamisbrug.[117] Principperne er udtryk for en generelt gældende grundsætning om *proportionalitet*, som indebærer, at indsamling, opbevaring og videregivelse af oplysninger som led i overvågning skal vurderes at være nødvendigt i forhold til overvågningens formål. Vurderingen bør omfatte en kvalitativ vurdering af, hvorvidt indsamling, opbevaring og anvendelse af den samlede mængde af oplysninger både er *egnet* og *nødvendig* for at realisere formålet med den iværksatte overvågning. EU-domstolens praksis indebærer, at der må stilles skærpede krav til denne proportionalitetsvurdering, hvis der er tale om mange oplysninger om mange borgere, og det ud fra de overvågede data er muligt at tegne en profil eller fastslå bevægelsesmønstre, da der i så fald er tale om en særlig indgribende type behandling.

Særligt i relation til ***myndighedsmæssig dataovervågning og samkøring*** kan databeskyttelsesrettens krav til rimelighed, lovlighed og gennemsigtighed samt princippet om formålsbegrænsning få særlig betydning. I en overvejende digital forvaltning kan der være legitim interesse i at genbruge, videregive og sammenstille oplysninger, der er indsamlet til ét formål, til brug for helt andre formål. [118] Fravigelse af princippet om, at personoplysninger kun må (gen)anvendes til de formål, hvortil de er indsamlet, kræver dog et klart retsgrundlag (f.eks. love, bekendtgørelser mv.), og at *det væsentligste indhold af de grundlæggende rettigheder og frihedsrettigheder* respekteres. Selvom der ikke er krav om direkte lovhjemmel, og der kan ske fravigelse af bl.a. pligten til at underrette borgerne om samkøringen, taler princippet om gennemsigtighed for , at der som minimum fastsættes specifikke bestemmelser om bl.a. formålene med behandlingen, rækkevidden af de indførte begrænsninger, opbevaringsperioder og gældende garantier under hensyntagen til behandlingens karakter, omfang og formål eller kategorier af behandling samt risiciene for de registreredes rettigheder. Sådan klarhed i retsgrundlaget kan fremme rimelighed og gennemsigtighed for borgerne, sikre demokratisk legitimitet og give grundlag for en kvalificeret samfundsdebat under lovgivningsprocessen.

Disse hensyn er bl.a. afspejlet i *den særlige parlamentariske proces,* der i 2018 blev indført i forhold til udnyttelse af bemyndigelsesbestemmelsen til administrativt at fastsætte regler, der fraviger princippet om formålsbegrænsning og oplysningspligt i forbindelse med *samkøring i kontroløjemed*. Fastsættelse af sådanne regler kræver således behandling i både Folketingets Retsudvalg og det relevante fagudvalg inden udstedelse af bekendtgørelsen, ligesom der i denne situation ikke er mulighed for generelt at undlade oplysningspligten overfor borgerne.[119] Tilsvarende kvalificerede krav til både indhold af retsgrundlag og proces for parlamentarisk behandling gælder imidlertid ikke

[117] Blume (2014) Overvågning. Kan persondataretten gøre nytte?
[118] Blume og Herrmann (2018) s. 312.
[119] Databeskyttelseslovens § 23.

for vedtagelse af lovgivning af samme karakter. Den nævnte særlige parlamentariske proces ved udstedelse af bekendtgørelser om samkøring er imidlertid ikke blevet anvendt en eneste gang, hvilket må tyde på, at samkøring i kontroløjemed besluttes gennem den almindelige lovgivningsproces.

Ved siden af de grundlæggende krav til rammerne for databehandling og karakteren af retsgrundlaget for behandling af oplysninger som led i overvågning gælder princippet om ansvarlighed (accountability). Ansvarlighedsprincippet er bl.a. afspejlet i reglerne om konsekvensanalyser, som må antages at indebære, at der gælder et krav om udarbejdelse af en konsekvensanalyse *inden* iværksættelsen af konkrete overvågningstiltag, som sandsynligvis vil indebære en høj risiko for borgernes rettigheder og frihedsrettigheder. Udarbejdelse af en sådan konsekvensanalyse er afgørende for at sikre et reelt fokus på borgernes rettigheder og frihedsrettigheder i forbindelse med indgribende og omfattende behandlinger af personoplysninger f.eks. som led i overvågning.

Rammerne for at iværksætte overvågning eller foretage samkøring eller profilering, hvorved der skabes et ret nærgående billede af den enkelte borgers private forhold, er i dag mere relevant end nogen sinde. Det er derfor vigtigt at overveje, hvilke rammer der skal gælde for brugen af sådan profilering. Det gælder navnlig i den offentlige sektor, hvor den enkelte borger ikke har mulighed for at vælge databehandlingen fra.

5 Udviklingen i overvågningstrykket

Indledningsvist redegøres der i afsnit 5.1 for tendensen til kraftig vækst i den myndighedsmæssige overvågning i Danmark. Herefter følger i afsnit 5.2 en kort gennemgang af udvalgte initiativer på EU-niveau. I afsnit 5.3 gennemgås en række konkrete begivenheder og tiltag, som over en 10-årig periode har haft betydning for retten til privatliv og beskyttelse af personoplysninger. Kapitlet afsluttes med en delkonklusion i afsnit 5.4.

5.1 Myndighedsovervågning i kraftig vækst

Justitia har siden sin oprettelse i 2014 haft særlig fokus på overvågningsområdet. I Justitias årlige statusrapporter om retssikkerheden i Danmark[120] nævnes hvert år udvalgte lovforslag og andre regeringsinitiativer, domme, rapporter og begivenheder, der i løbet af det pågældende år har haft betydning for udviklingen i beskyttelsen af grundlæggende retsstatsprincipper og menneskerettigheder i Danmark. Selvom der ikke er tale om en udtømmende eller fuldstændigt dækkende gennemgang af samtlige relevante tiltag, er overvågningsområdet et af de områder, som er blevet fulgt tæt. Institut for menneskerettigheder følger ligeledes overvågningsområdet tæt både i deres årlige opsamlende rapporter og diverse temarapporter.

Et tilbageblik på bl.a. disse rapporter giver et klart indtryk af, at den myndighedsmæssige overvågning er i kraftig vækst, og at overvågningen favnes som et redskab til at sikre kontrol og øget effektivitet mv. Et karakteristisk eksempel på dette er loven om *forbud* mod tv-overvågning, som skiftede navn til lov om tv-overvågning i 2008, da privates adgang til at videoovervåge endnu en gang blev udvidet. Som en afledt konsekvens heraf blev politiets adgang til sådanne optagelser i efterforskningsmæssig sammenhæng - ligesom andre offentlige myndigheders videoovervågning - reguleret i loven med henblik på at give politiet øgede muligheder for at overvåge i kriminalitetsbekæmpende øjemed.[121]

Navnlig fra 2010 og frem har der været retssikkerhedsmæssige bekymringer i forhold til almindelige kontrolmyndigheders øgede adgang til bredspektret indhentning af oplysninger som led i effektivisering og målretning af deres indsatser. Både Justitia og Institut for Menneskerettigheder[122] har derfor haft fokus på, om skattemyndighedernes og andre offentlige myndigheders øgede adgang til bredspektret indhentelse af personoplysninger i samkøringsøjemed til brug for kontrolindsatser – herunder oplysninger som teledata, rejseaktivitet mv., som oprindeligt er indsamlet af andre aktører til helt andre formål - kunne være i strid med grundlæggende rettigheder om beskyttelse af privatliv og personoplysninger, bl.a. som følge af uklare retsgrundlag og brede

[120] Rapporterne fokuserer særligt på Justitias fokusområder; frihedsrettigheder, grundlæggende menneskerettigheder, retsstatslige principper samt borgeres og virksomheders retssikkerhed.
[121] Lov nr. 519 af 6. juni 2007 og tv-overvågningsudvalgets bemærkninger til lovforslaget §1, nr.1 i betænkning nr. 1483/2006.
[122] Se f.eks. Institut for Menneskerettigheders rapport om Forvaltningens kontrol, status 2015-2016.

myndighedsmæssige skøn, der ikke i fornødent omfang kan anses for at beskytte borgerne mod vilkårlige indgreb i beskyttelsen af privatliv og personoplysninger.

Særligt udviklingen af ny teknologi og analyseværktøjer har givet appetit på at effektivisere og automatisere. Med etableringen af Udbetaling Danmark i 2012 begyndte udviklingen for alvor at accelerere med stadigt mere omfattende beføjelser til behandling af personoplysninger, og en større og større mængde oplysninger til kontrolindsatsen mod fejl og snyd med sociale ydelser. Justitia har udarbejdet flere kritiske analyser, som har sat fokus på, om Udbetaling Danmarks beføjelser er forenelige med beskyttelsen af borgernes grundlæggende rettigheder og retssikkerhed [123] Tilsvarende konklusioner ses også i rapporter udarbejdet af Institut for Menneskerettigheder og Amnesty International. [124] Der har også internationalt været opmærksomhed på området fra organisationer som f.eks. Algorithm Watch,[125] hvilket ikke mindst skyldes, at der i praksis opstår en social slagside i forhold til overvågningstiltag målrettet personer, der modtager sociale ydelser. Samtidig har udbyttet af den meget omfattende overvågning ofte vist sig at være meget beskedent eller ligefrem ført til rejsning af kontrolsager på urigtigt grundlag. Algorithm Watch offentliggjorde i 2020 en stor undersøgelse af erfaringer med automatiseret eller beslutningsunderstøttende algoritmer i 16 EU-lande, herunder Danmark. I den forbindelse afdækkede man flere alvorlige eksempler på, hvordan algoritmer til systematiske samstillinger af personlige oplysninger anvendt af myndigheder kunne føre til forkerte resultater og dermed alvorlige krænkelser af borgeres rettigheder, når de på baggrund af en automatiseret proces blev inddraget i myndighedernes 'suspicion-machine'.[126]

Den stigende anvendelse af teknologiske løsninger og algoritmer, der overvåger millioner menneskers data for at finde de få, er med til at øge overvågningstrykket. Samtidig er der begrænset indsigt i algoritmernes opsætning og vægtninger.[127] Der har været stort politisk fokus på disse afledte retssikkerhedsmæssige problemstillinger i 2024.[128]

5.2 Initiativer på EU-niveau

EU har gennem tiden haft særlig fokus på at beskytte behandling og anvendelse af borgernes oplysninger og at arbejde for begrænsning af overvågning til beskyttelse af de grundlæggende

[123] Justitia (2015): Udbetaling Danmark: En trussel mod privatlivets fred og retten til databeskyttelse 'Udbetaling Danmarks systematiske overvågning' (2019).
[124] Amnesty International (2024) Coded Injustice: Surveillance and Discrimination in Denmark's automated welfare state.
[125] Algorithm Watch er en uafhængig, non-profit organistation, baseret i Berlin og Zurich, som holder øje med, hvordan algoritmer anvendes på et europæisk plan uden at svække retssikkerhed, menneskerettigheder og demokratiske værdier. www.algorithmwatch.org.
[126] Algorithm Watch (2020) Automating Society.
[127] Se FOB2022-23 hvor Folketingets ombudsmand ikke fandt at kunne tilsidesætte Udbetaling Danmarks vurdering af, at væsentlige hensyn til gennemførelse af offentlig kontrol gjorde det nødvendigt at undtage oplysninger om model. Se også artikel i Radar om samme emne: https://radar.dk/artikel/juridisk-direktoer-vil-undgaa-mytedannelse-men-fastholder-lukketheden-om-skats-ai-profilering.
[128] Folketingsbeslutning 2023/1 BSF 136 fremsat 29. februar 2024 af SF om at pålægge regeringen at fremsætte et lovforslag, der sikrer, at danske myndigheders brug af algoritmer sker efter principper om transparens og forklarlighed.

rettigheder. Det gælder eksempelvis Databeskyttelsesforordningen (GDPR)[129], AI forordningen[130] og E-privacy reguleringen.[131] Derudover har EU-domstolen været meget aktiv i forhold at fortolke proportionalitetsprincippet i forhold til generel og udifferentieret registrering og opbevaring (logning) af den brede befolknings teledata og har gennem praksis statueret, at der gælder et forbud mod generel og udifferentieret logning af teledata med henblik på bekæmpelse af grov kriminalitet, og stillet krav om, at en sådan logning kun kan ske i situationer, hvor medlemsstaten står over for en alvorlig trussel mod den nationale sikkerhed, som må anses for at være reel og aktuel eller forudsigelig. Domstolen har også i en række andre sager taget stilling til de øvrige betingelser, der skal være opfyldt for at gøre indgreb i retten ti beskyttelse af privatliv og personoplysninger. Se ovenfor i afsnit 3.2.3 om relevant praksis fra EU-domstolen.

I de senere år har der imidlertid også været flere eksempler på EU-lovgivningsinitiativer, der omvendt har bidraget til at øge overvågningstrykket. Her kan bl.a. nævnes Digital Services Act (DSA) [132] og Europa-kommissionens CSA-forordning med forslag til chatcontrol,[133] som begge indeholder skrappe krav til udbydere af sociale medier om at moderere brugernes indhold, som medfører risiko for omfattende censur, men også forudsætter en omfattende privatretlig overvågning af indholdet på platformene. Derudover kan nævnes direktivet om passagerlisteoplysninger (PNR-direktivet),[134] som forudsætter, at flyselskaber indsamler og systematisk videregiver oplysninger om flypassagerer til brug for bekæmpelse af grov kriminalitet samt et tilsvarende direktiv vedrørende skibspassagerer.[135] Disse oplysninger blev oprindeligt besluttet indsamlet og opbevaret af hensyn til terrorbekæmpelse, men formålet er med årene blevet udvidet til også at omfatte grov kriminalitet, ligesom oplysningerne kan anvendes til kriminalitetsanalyse. PNR-direktivet er gennemført i dansk ret via PNR-loven fra 2018,[136] som i et vist omfang præciserer, hvilke oplysninger der indsamles, og hvilke rammer der gælder for den videre anvendelse.

---

[129] 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 mv. (GDPR).
[130] Europa-Parlamentets og Rådets forordning (EU) 2024/1689 af 13. juni 2024 om harmoniserede regler for kunstig intelligens mv. Forordningen trådte i kraft 1. august 2024.
[131] EU direktiv 2002/58 af 12. Juli 2001 om behandling af personoplysninger og beskyttelse af privatlivets fred i den elektroniske kommunikationssektor (e-privacy direktivet) samt forslag til Europa-Parlamentets og Rådets forordning om respekt for privatliv og beskyttelse af personoplysninger i forbindelse med elektroniske kommunikation og om ophævelse af direktiv 2002/58/EF.
[132] Se Justitias analyse fra 2022 herom: https://futurefreespeech.com/wp-content/uploads/2022/05/Report_thoughts-on-DSA.pdf.
[133] CSA forordningen forhandles fortsat, men Europa-Parlamentet og Rådet har henholdsvis den 10. og 29. april 2024 vedtaget midlertidige ændringer af forordning nr. 2021/1232, som gælder frem til den 20. april 2026, hvor CSA-forordningen forventes at være vedtaget og trådt i kraft.
[134] EU-Parlamentets og Rådets direktiv nr. 2016/681 af 27. april 2016 om anvendelse af passagerlisteoplysninger til at forebygge, opdage, efterforske og retsforfølge terrorhandlinger og grov kriminalitet (PNR-direktivet).
[135] Direktiv (EU) 2017/2109 om ændring af Rådets direktiv 98/41/EF om registrering af de ombordværende på passagerskibe.
[136] Lov nr. 1706 af 27. december 2018, som senere *ændret* i 2021, 2022 og 2024.

5.3 Konkrete påvirkninger af retten til privatliv

Tidslinjen nedenfor indeholder eksempler på konkrete begivenheder, tiltag, og faktuelle forhold, der påvirker retten til privatliv og beskyttelse af personoplysninger. Formålet er at illustrere udviklingen i tiltag, der i perioden 2014-2024 har påvirket overvågningstrykket i Danmark. Det gælder både tiltag som henholdsvis har øget og reduceret overvågningstrykket.

Tidslinjen er udfærdiget på baggrund af Justitias årlige statusrapporter, temaanalyser samt lignende udgivelser fra andre organisationer. Der er således ikke tale om en udtømmende liste, men en liste over relevante begivenheder, som på forskellig måde er kommet til Justitias kendskab gennem årene.

2014

Center for Cybersikkerhed (CFCS) blev oprettet som en enhed under Forsvarets Efterretningstjeneste (FE) med vidtgående muligheder for overvågning.[1]

Politiet begynder at anvende automatisk nummerpladegenkendelsesteknologi (ANPG).[2]

Finansielle virksomheder får udvidet adgang til oplysninger fra Indkomstregistret, hvilket øger mængden af persondata, som de kan indsamle.[3]

EU-domstolen erklærer EU's direktiv om pligtmæssig logning af teleoplysninger for ugyldigt, da generel og udifferentieret logning af borgernes teleoplysninger strider mod retten til beskyttelse af privatlivets fred og beskyttelse af personoplysninger.[4]

Politiet får øgede kontrolmuligheder ved hjælp af fly- og skibspassageroplysninger samt ANPG ved grænseområder.[5]

2015

Udbetaling Danmarks beføjelser og samstillingsadgange udvides yderligere med henblik på effektivisering af kontrol med fejl og snyd med sociale ydelser.[6]

Rigsrevisionen sætter fokus på effektiviteten af datasamkøringer i kontroløjemed i samarbejdet mellem Udbetaling Danmarks og kommunerne.[7]

Justitia sætter fokus på Udbetaling Danmarks omfattende beføjelser med analysen *Udbetaling Danmark: En trussel mod privatlivets fred og retten til databeskyttelse.* [8]

Forsvarets Efterretningstjeneste får udvidet mulighederne for målrettet overvågning af danskere i udlandet uden retskendelse.[9]

Skatteministeren standser Skats indhentning af teleoplysninger uden kendelse til brug for skattekontrollen efter samfundsmæssig debat.[10]

Nedlægning af Terrorkommissionen, som bl.a. havde til formål at vurdere, om der fandtes elementer i de vedtagne terrorpakker, som var for vidtgående i forhold til bl.a. overvågning af befolkningen.[11]

Arbejdstilsynet får adgang til at indhente oplysninger fra eksterne registre til kontrolindsatsen.[12]

Bekendtgørelse muliggør, at politiet ved anvendelse af ANPG bl.a. kan opbevare 'no-hits' i op til 30-dage.[13]

2016

Regeringen planlægger genindførelse af sessionslogning, mens teleoplysninger fortsat logges.[14]

SikkerhedsBranchen anslår, at der er ca. 1,5 millioner tv-overvågningskameraer installeret i Danmark. Tallet var 500.000 i 2013.[15]

Der oprettes mulighed for kommunalt tilskud til privat tv-overvågning.

Institut for Menneskerettigheder sætter i temarapport fokus på, om forvaltningens kontrol er forenelig med de grundlæggende rettigheder.[16]

EU-domstolen fastslår, at EU's charter om grundlæggende rettigheder er til hinder for regler om generel og udifferentieret lagring (logning) af samtlige borgeres trafik- og lokaliseringsdata mv. (sessionslogning) til brug for kriminalitetsbekæmpelse.[17] Herefter udskydes regeringens planer om genindførelse af sessionslogning, mens revision af de generelle logningsregler udskydes på ny.[18]

2017

Forslag til ny databeskyttelseslov giver offentlige myndigheder udvidet adgang til administrativt at samkøre personoplysninger om borgerne i kontroløjemed.[19]

Erhvervsstyrelsen fremsætter forslag til lov om deling af data, der giver styrelsen udvidet adgang til oplysninger fra Skat og andre myndigheder.[20]

Politiets og Forsvarets efterretningstjenester får hurtigere adgang til personoplysninger om udlændinge i sikkerhedsarbejdet.[21]

Folketinget vedtager lov om Forsvarets Efterretningstjenestes personoplysninger, der giver FE adgang til oplysninger om flypassagerer via Skat uden dommerkendelse.[22]

Politiet begynder at anvende POL-INTEL og får adgang til oplysninger om flypassagerer via Skat uden retskendelse.[23]

Politiets muligheder for at anvende ANPG udvides.[24]

Nyt EU-direktiv opdaterer kravene til optælling og registrering af passagerer og besætning om bord på passagerskibe, som skal indrapporteres til nationale myndigheder.[25]

Fyns Politi begynder at anvende droner i deres arbejde som en testordning.[26]

Forslag til ny skattekontrollov med omfattende hjemler til terminaladgang og samkøring på tværs af både interne og eksterne registre hos andre offentlige myndigheder.[27]

Justitia sætter med analysen *Ny skattekontrollov – Har Skatstadig adgang til fortrolige teleoplysninger* fokus på, at Skats retsgrundlag for samkøring stadig er uklart.[28]

2018

EU's databeskyttelsesforordning (GDPR) afløser persondataloven og skærper kravene til ansvarlighed og gennemsigtighed ved behandling af borgernes data.[29]

Den supplerende danske databeskyttelseslov udvider mulighederne for genanvendelse af data ved at fjerne hidtidige krav om direkte lovhjemmel ved samkøring i kontroløjemed.[30]

Erhvervsstyrelsen får udvidet muligheder for at indsamle og behandle (herunder samkøre) oplysninger til kontrol- og tilsynsopgaver.[31]

Lov om indsamling, anvendelse og opbevaring af oplysninger om flypassagerer (PNR-oplysninger) vedtages, hvilket øger indsamling og deling af borgeres oplysninger.[32]

Gladsaxe Kommune planlægger at bruge algoritmer til at identificere borgere med risiko for sociale problemer. Projektet skrinlægges efter massiv kritik for at krænke privatlivets fred.[33]

Hjemmel til samkøring af CPR-registret, BBR-registret og Det Fælleskommunale Ejendomsregister med henblik på kontrol af overholdelse af bopælspligt.[34]

Mulighed for kommuners indhentning af oplysninger fra forsyningsselskaber om elforbrug til kontrol af bopælspligten opgives efter samfundsmæssig debat.[35]

Ny lov om aktiv beskæftigelsesindsats introducerer et værktøj, der samkører data om borgere for at finde potentielle langtidsledige.[36]

Mulighederne for, at erhvervsdrivende kan dele videoovervågningsmateriale mellem sig, udvides.[37]

Politiet tildeles 150 videokameraer ved finanslovsforhandlingerne til brug for en særlig tryghedsskabende indsats i det offentlige rum.[38]

2019

Regeringen fremlægger Trygheds- og sikkerhedspakken med initiativer til øget privat og offentlig videoovervågning bl.a. for at fremme trygheden og til brug for et bredt kriminalitetsbekæmpelseshensyn. Politiet får flere midler til tryghedsskabende overvågning i det offentlige rum. Politiet får mulighed for at overtage tv-overvågning i

realtid i ekstraordinære situationer med henblik på at forebygge eller efterforske kriminalitet.[39]

Københavns Politi udtaler til medie, at de ønsker at benytte ansigtsgenkendelsesteknologi til kriminalitetsbekæmpelse.[40]	
Justitia sætter fokus på henholdsvis Udbetaling Danmarks systematiske dataovervågning[41] og kommunernes efterfølgende kontrol med modtagere af sociale ydelser.[42]	
Straffeloven ændres så dømte seksualforbrydere underlægges strengere kontrol efter endt afsoning. Ændringen indeholdt bl.a. mulighed for politiet til at føre tilsyn med den dømtes bolig, breve og andre papirer uden retskendelse. Tilsynet kunne foretages jævnligt, uanmeldt og på vilkårlige tidspunkter.[43]	
Teledatasagen ruller, hvor politiet har anvendt fejlbehæftede teledata i straffesager. 10.000 afsluttede straffesager skal undersøges.[44]	
Udvikling af datadrevet profileringsværktøj gennem samkøring af personoplysninger til brug for kommunernes risikovurdering af langtidsledige.[45]	
Ændringsforslag til skattekontrollovsforslaget fra 2017 med tilføjelse om begrænsning af anvendelse af teleoplysninger.[46]	

2020

	EU-domstolen fastslår, at generel og udifferentieret lagring af teledata kan indføres tidsbegrænset, ved alvorlig trussel mod den nationale sikkerhed, der er reel og aktuel eller forudsigelig. EUD fastslog også, at nationale logningsregler ikke kan opretholdes midlertidigt, når de strider mod EU-retten. [47]
	Danske myndigheder tilbyder kontaktsporingsapp i forbindelse med bekæmpelse af covid-smitte under pandemien.[48]
	Politisk aftale vil etablere digital patruljeenhed, som skal overvåge åbne grupper på sociale medier mv.[49]
	Signaturprojekter med kunstig intelligens i kommuner og regioner igangsættes, hvor kommuner og regioner får offentlige midler til at afprøve kunstig intelligens i forvaltningen.[50]
	Markante udvidelser i privates og offentlige myndigheders adgang til videoovervågning efter tv-overvågningsloven, bl.a. i forhold til hvem der må videoovervåge, hvor meget af det offentligt tilgængelige areal, overvågningen må omfatte og hvor længe optagelserne må opbevares. Kommuner får mulighed for at videoovervåge for at fremme trygheden. Registrering i politiets videoovervågningsregister gøres obligatorisk.[51]
	Politiets anvendelse af droner reguleres.[52]

2021

Justitia udgiver rapporten Ulovlig logning – Tid til en lovrevision, hvor Justitsministeriet håndtering af lognings-området kritiseres, særligt opretholdelsen af den ulovlige logning. [53]

Udvidelse af Skats muligheder for datasamkøring med henblik på anvendelse af kunstig intelligens og Machine Learning i skattekontrollen og som led i udvikling af profileringsmodeller.[54]

Rigsrevisionens undersøgelse af politiets tryghedsskabende videoovervågning afdækker, at kriterierne for at opsætte kameraerne er meget uklare.[55]

2022

Nye regler for slettefrister vedrørende DNA-profiler og fingeraftryk udvider muligheden for tættere profilering af borgere.[56]

Politiet begynder at anvende ansigtsgenkendelsesteknologi i forbindelse med digital offergenkendelse i sager om seksuelt misbrug af børn.[57]

Nye logningsregler træder i kraft, der fortsat giver mulighed for generel og udifferentieret logning af teleoplysninger, hvilket igen kritiseres for at krænke privatlivets fred.[58]

Digital Services Act (DSA) vedtages og medfører, at sociale medier aktivt skal overvåge deres platform for ulovligt indhold.[59]

Opbevaring af 'no-hits' fra politiets stationære ANPG-overvågning udvides til 60 dage og til 7 dage fra mobile enheder. Samtidig lempes kravene til, hvornår de må anvendes ANPG.[60]

EU-domstolen fastslår, at teledata, som er logget af hensyn til en national sikkerhedstrussel, ikke kan bruges af politiet i sager af mindre alvorlighed end national sikkerhed.[61]

Ændring af de danske logningsregler, og der indføres tidsbegrænset logning på baggrund af en konkret trusselsvurdering mod den nationale sikkerhed.[62]

Indførelse af generel og udifferentieret registrering og opbevaring af oplysninger om en slutbrugers adgang til internettet (begrænset sessionslogning).[63]

2023

Højesteret træffer i en konkret straffesag kendelse om, at teleoplysninger, som er logget og indhentet i strid med EU-retten, kan anvendes som bevis i sagen.[64]

Regeringen tilslutter sig beslutningsforslag om dansk politi skal kunne bruge genetisk slægtsforskning i efterforskning.[65]	
CSA-forordning er på tegnebrættet og indeholder bl.a. Chatkontrol, som vil medføre overvågning af al digital kommunikation i EU-lande.[66]	
Forlængelse af tidsbegrænset logning på baggrund af en konkret trusselsvurdering.[67]	

2024

	Markant udvidelse af, hvor stor en andel af det offentligt tilgængelige areal, som privates og offentlige myndigheders videoovervågning må omfatte efter tv-overvågningsloven. Den i 2020 lovede evaluering udskydes i 2 år.[68]
	Nye regler om logning træder i kraft. Selvom loven er blevet indskrænket, kritiseres den stadig for at være bredere, end det er lovligt ifølge EU-domstolens praksis.[69]
	Flere politikredse begynder at anvende kropskameraer i udvalgte operationer.[70]
	AI-forordningen vedtages i EU, som bl.a. regulerer anvendelsen af ansigtsgenkendelsesteknologi og højrisiko-AI.[71]
	Justitia sætter fokus på behovet for at regulere politiets anvendelse af ansigtsgenkendelse, herunder retssikkerhedsmæssige betænkeligheder ved anvendelse uden kendelse mv.[72]
	Politisk aftale medfører, at politiet får mulighed for at anvende ansigtskendelsesteknologi i forbindelse med opklaring af sager om alvorlig personfarlig kriminalitet som f.eks. drab, forsøg på drab, grov vold, voldtægt og lignende overtrædelser. Anvendelsen må kun anvendes bagudrettet og ikke i realtid.[73]
	Aktindsigt viser, at Skattestyrelsen bruger 23 forskellige AI-systemer til at bearbejde borgernes personlige oplysninger, og at 6 AI-systemer er under udvikling.[74]
	Lovforslag fremsættes som muliggør anvendelsen af omvendt elektronisk fodlænke til støtte af opretholdelsen af visse typer opholdsforbud.[75]
	Ny forlængelse af tidsbegrænset logning på baggrund af en konkret trusselsvurdering.[76]
	Lovforslag fremsættes som muliggør, at butikker gerne må lave aflytning og lydoptagelser af både kunder og medarbejdere, så længe det fremgår tydeligt.[77]

Noter til tidslinjen kan findes under afsnit 9.1 til sidst i rapporten.

5.4 Delkonklusion

Et tilbageblik på overvågningstiltag i Danmark de seneste 10 år giver et klart indtryk af, at den myndighedsmæssige overvågning er i kraftig vækst, og at overvågningen favnes som et redskab til at sikre kontrol og øget effektivitet mv.

Navnlig fra 2010 og frem har der fra flere sider været udtrykt retssikkerhedsmæssige bekymringer i forhold til kontrolmyndigheders øgede adgang til bredspektret indhentning af oplysninger som led i effektivisering og målretning af kontrolindsatsen. Alligevel er kontrolbeføjelserne flere gange blevet udvidet, hvilket sammen med de øgede teknologiske muligheder har lagt et større og større pres på overvågningstrykket.

EU har gennem årene haft særlig fokus på beskyttelse af personoplysninger, og EU-domstolen har tilsvarende været aktiv i forhold til fortolkning af rettighederne og i forhold til den proportionalitetsvurdering, som er central for vurderingen af, om et overvågningstiltag er foreneligt med de EU-retlige grundprincipper for beskyttelse af privatliv og personoplysninger.

Særligt de seneste år har der dog også været modsatrettede tendenser. Selvom lovgivningsinitiativerne har haft fuldt ud legitime formål og bl.a. tilsigter at styrke sikkerheden i EU samt at bekæmpe terror og anden kriminalitet mv., kan initiativerne i praksis medvirke til at indskrænke borgernes frihedsrettigheder. Det gælder i særlig grad ytringsfriheden, som er under et stadigt stigende pres i kampen mod hate-speech, digitale seksualkrænkelser og misinformation af offentligheden. I takt med, at overvågningsredskaberne bliver mere og mere effektive, er der en tendens til, at overvågningsintensiteten tilsvarende øges.

6 Videoovervågning

I afsnit 6.1 nedenfor redegøres der for tendensen til og baggrunden for den øgede videoovervågning i det offentlige rum. Derefter ses der i afsnit 6.2 kort på effekten af videoovervågning i forhold til kriminalitet. I afsnit 6.3-6.5 ses nærmere på udviklingen i henholdsvis tv-overvågningsloven, politiets overvågning med ANPG og politiets tryghedsskabende videoovervågning. Kapitlet afsluttes med en delkonklusion i afsnit 6.6.

6.1 Øget videoovervågning i det offentlige rum

Der kan næppe være tvivl om, at det samlede videoovervågningstryk i det offentlige rum er stigende. Både private aktører og offentlige myndigheder, herunder politiet, overvåger i langt videre omfang end tidligere i det offentlige rum. Organisationen Sikkerhedsbranchen har i 2016 estimeret, at der findes omkring 1,5 millioner kameraer i Danmark.[137] Sikkerhedsbranchen har ikke noget nyere estimat, men det må forventes, at tallet er væsentligt højere i dag, bl.a. fordi prisen på udstyret er lavere og kan købes i den almindelige detailhandel. [138]

Stigningen kan være forbundet med de nutidige fleksible retlige rammer. Det er eksempelvis muligt for kommunerne at videoovervåge offentligt tilgængelige steder, der ligger i tilknytning til en restaurationsvirksomhed eller på offentligt tilgængelige arealer tæt på boligområder, hvor bl.a. boligforeninger med politiets tilladelse foretager overvågning ud fra væsentlige hensyn til kriminalitetsbekæmpelse. Kriteriet for kommunernes videoovervågning er imidlertid ikke, at det skal være af væsentlige hensyn til kriminalitetsbekæmpelse, men at det vurderes at 'fremme trygheden'.[139]

Politiet har fået vide beføjelser til at stille krav til, hvor og hvordan der af kriminalitetsbekæmpelseshensyn skal videoovervåges i det offentlige rum, ligesom politiet i flere tilfælde er den kompetente myndighed i forhold til at give private tilladelse til at foretage videoovervågning.[140] Politiet kan derudover henstille til private samt direkte pålægge offentlige myndigheder at foretage videoovervågning indenfor rammerne af lovgivningen.[141]

---

[137] Berlingske. Video stopper tyven - men vold forhindrer overvågning ikke. 8. december 2016, https://www.berlingske.dk/samfund/video-stopper-tyven-men-vold-forhindrer-overvaagning-ikke.
[138] Samtidig er den mobile private kameraovervågning formentlig i hastig fremgang, bl.a. som følge af integrationen i Teslas biler, som er blandt de mest solgte elbiler i Danmark, se f.eks. https://mobilsiden.dk/nyheder/opkoblede-biler/top-6-de-mest-solgte-elbiler-i-2024/, https://mobility.dk/nyregistreringer/ og https://fdm.dk/nyheder/nyt-om-biler/2023-12-elektrisk-revolution-tesla-slaar-37-aar-gammel-salgsrekord.
[139] Tv-overvågningslovens § 2a, jf. § 2, stk.2, § 2 c, stk. 1 og stk. 3. Se også Lov 2020-06-09 nr. 802 om ændring af lov om tv-overvågning. Se også lovforslaget LFF 2020-02-05 nr. 102 om ændring af tv-overvågningsloven (Styrkelse af trygheden og sikkerheden, herunder udvidelse af adgangen til tv-overvågning for private og offentlige myndigheder samt obligatorisk registrering af tv-overvågning) for overvejelserne bag lovændringen.
[140] Tv-overvågningslovens § 2, stk. 1, nr. 4 og 5, jf. § 2, stk. 6. og § 2, stk. 2.
[141] Tv-overvågningslovens § 2d.

Private virksomheder, offentlige myndigheder, foreninger mv. har desuden pligt til at lade sig registrere i Politiets Kameraregister over tv-overvågningskameraer (POLCAM) samt indberette eventuelle væsentlige ændringer.[142] Antallet af registreringer i POLCAM udgjorde i 2023 i alt 38.388, som reelt kan dække over et langt større antal kameraer, da registreringen omfatter en adresse med et eller flere kameraer.[143]

Politiet har på flere måder en særstatus i forhold til øvrige offentlige myndigheders anvendelse af videoovervågning, hvilket selvfølgelig skyldes, at politiet varetager en meget væsentlig samfundsmæssig opgave med at forebygge og efterforske kriminalitet. Navnlig i forhold til efterforskning kan videoovervågning være særdeles effektivt. Udover at være godkendende instans i forhold til øvrige offentlige myndigheders og privates videoovervågning efter tv-overvågningslovens regler, anvender politiet også selv videoovervågning som led i deres opgavevaretagelse.

Når politiet iværksætter **videoovervågning af personer, der befinder sig på et *ikke-frit tilgængeligt sted***, skal det ske efter retsplejeloven regler om observation, hvilket bl.a. forudsætter rettens tilladelse. [144] Politiets efterforskningsmæssige beslutninger om at iværksætte **videoovervågning på *frit tilgængeligt sted*** som led i efterforskning af strafbare forhold kan derimod ske uden rettens godkendelse og alene på baggrund af en almindelig, ulovbestemt proportionalitetsvurdering. [145] Politiets behandling af oplysninger skal i den sammenhæng ske indenfor rammerne af de generelle regler i retshåndhævelsesloven.[146] Det ses imidlertid ikke afklaret i praksis, hvor konkret og alvorligt efterforskningsmæssigt behov, der skal være tale om, for at en mere bredspektret overvågning som led i et generelt kriminalitetsbekæmpelseshensyn kan anses for proportionelt og foretages indenfor rammerne af retshåndhævelsesloven. Tilsvarende gælder for videoovervågning med et *tryghedsskabende* sigte.

De seneste 5-6 år har det været en udtalt politisk prioritet generelt at sætte ind med styrket overvågning i det offentlige rum. Det politiske udspil 'Tryghed og Sikkerhed i det offentlige rum' fra 2019 omfatter således både udvidelser indenfor tv-overvågningsloven for privates og offentlige

[142] Jf. tv-overvågningslovens § 2e, som trådte i kraft den 1. juli 2021, jf. bekendtgørelse 2021-05-28 nr. 1060 om ikrafttræden af § 1, nr. 10, i lov om ændring af lov om tv-overvågning (Styrkelse af trygheden og sikkerheden, herunder udvidelse af adgangen til tv-overvågning for private og offentlige myndigheder samt obligatorisk registrering af tv-overvågning). Se også lov 2020-06-09 nr. 802 om ændring af lov om tv-overvågning og lovforslaget LFF 2020-02-05 nr. 102 om ændring af tv-overvågningsloven (Styrkelse af trygheden og sikkerheden, herunder udvidelse af adgangen til tv-overvågning for private og offentlige myndigheder samt obligatorisk registrering af tv-overvågning) for overvejelserne bag lovændringen punkt 2.1.2.1.
[143] Besvarelse af spørgsmål nr. 812 til Folketingets Retsudvalg af 18. april 2024.
[144] Retsplejelovens § 780.
[145] UfR 2021.1262.
[146] Lov nr. 410 af 27. april 2017 om retshåndhævende myndigheders behandling af personoplysninger, som regulerer politiets behandlinger af personoplysninger med henblik på at forebygge, efterforske, afsløre eller retsforfølge strafbare handlinger mv.

myndigheders overvågning, politiets overvågning med automatisk nummerplade-genkendelsesteknologi (ANPG) samt politiets tryghedsskabende overvågning.[147]

Det politiske udspil var umiddelbart begrundet i en række voldsomme eksplosioner i et offentlige rum og øget aktivitet i bandemiljøet. Statsminister Mette Frederiksen udtalte bl.a. følgende til medierne:

"Vi ser en rigtig grim og grov kriminalitet i vores samfund, som i høj grad relaterer sig til banderne og den organiserede kriminalitet. Jeg synes, de har fået for godt fat i vores samfund, og det ønsker jeg selvfølgelig ikke'."[148]

Den politiske intention var at give mulighed for at *'overvåge bredere og ikke kun snævert."*[149]

Den teknologiske udvikling har samtidig betydet, at videoovervågning i endnu højere grad end tidligere kan anvendes til at skabe meget nærgående profiler af de enkelte personer ved, at der kombineres med teknologier som ansigtsgenkendelse og andre analytiske redskaber. Dette kan udgøre et særligt intensivt indgreb i privatlivets fred, idet denne kombination af teknologiske muligheder gør det med EU-domstolens ord muligt *'at drage meget præcise slutninger vedrørende privatlivet for de omfattede personer, såsom vaner i dagligdagen (...) sociale relationer og sociale miljøer, de frekventerer.'* [150]

6.2 Effekten af videoovervågning

Kriminalitetsbekæmpelse er uden tvivl et legitimt formål, og kan i henhold til de menneskeretlige regler accepteres som indgreb i de grundlæggende rettigheder, hvis der foreligger et aktuelt kriminalitetsmæssigt problem det sted, der skal videoovervåges, og videoovervågningen er af en sådan karakter, at den utvivlsomt vil være virksom i forbindelse med bekæmpelsen af denne kriminalitet.[151]

Videoovervågning kan være meget værdifuldt i en *efterforskningsmæssig* sammenhæng. Derimod har videoovervågning meget sjældent et dokumenteret *kriminalitetsforebyggende* sigte. Det Kriminalpræventive Råd har flere gange peget på, at videoovervågning kun har en dokumenteret forebyggende effekt i nogle helt bestemte situationer som f.eks. hærværk og indbrud i parkeringskældre, og at den forebyggende virkning på den objektive utryghed, altså den enkelte borgers reelle udsathed i forhold til at blive ramt af kriminalitet, derimod må anses for meget lav i

[147] 'Tryghed og Sikkerhed i det offentlige rum' (2019), afsnit 4 'Politiet styrker brugen af videoovervågning'. https://www.regeringen.dk/media/7435/tryghed-og-sikkerhed-i-det-offentlige-rum.pdf.
[148] https://nyheder.tv2.dk/samfund/2019-10-08-statsministeren-varsler-massivt-oeget-overvaagning-i-danmark.
[149] TV2 Nyheder: https://nyheder.tv2.dk/samfund/2019-10-08-statsministeren-varsler-massivt-oeget-overvaagning-i-danmark.
[150] La Quadrature du Net-dommen, EUD af 6. oktober 2020 (forenede sager C-511/18, C-512/18 og C-520/18), præmis 117. Dommen vedrørte generel og udifferentieret logning af tele- og lokationsdata.
[151] EUD af 11. december 2019, Case of TK (C-708/18), præmis 46-47.

forhold til den type personfarlig kriminalitet, som i mange tilfælde har udløst ønsket om at skabe tryghed. [152]

En omfattende meta-analyse foretaget af BRÅ, det svenske kriminalpræventive råd, i 2019, viser samme resultat .[153] Analysen omfattede over 80 forsøg[154] i forskellige lande, som undersøgte, om videoovervågning havde en forebyggende effekt på kriminalitet. Resultatet var, at der ikke kunne påvises nogen forebyggende effekt i forhold til personfarlig kriminalitet, men en vis forebyggende effekt i forhold tyveri fra parkeringskældre og lignende.

I forhold til *oplevet, subjektiv utryghed* har Det Kriminalpræventive Råd i stedet peget på andre relevante indsatser i udfordrede lokalområder, f.eks. af fysisk karakter. Rådet har i forbindelse med høringer over lovforslag udtrykt generel betænkelighed ved øget videoovervågning i det offentlige rum.[155]

6.3 Udviklingen i tv-overvågningsloven

6.3.1 Den første regulering og udvikling

I 1982 blev privates adgang til at foretage videoovervågning på frit tilgængelige områder for første gang reguleret i en særlig lov.[156] Loven blev formuleret som et generelt forbud mod privates videoovervågning, da det blev vurderet at virke krænkende, hvis en udbredt anvendelse af overvågningsudstyr begrænsede mulighederne for at kunne færdes på frit tilgængelige områder uden at blive udsat for skjult iagttagelse eller fotografering.[157] Der blev derfor også kun gjort enkelte undtagelser til 1982-lovens forbud, som ifølge lovteksten alene var møntet på at regulere privates tv-overvågning.

Offentlige myndigheders tv-overvågning var i første omgang ikke omfattet af loven og var alene reguleret af et ulovbestemt proportionalitetsprincip i forhold til det, der blev betragtet som et væsentligt myndighedsmæssigt indgreb i borgernes privatliv. Ifølge tv-overvågningsudvalget var der i 1982 en udbredt opfattelse af, at overvågningsapparatur ville begrænse borgernes mulighed for at færdes på frit tilgængelige områder uden at være udsat for skjult iagttagelse eller fotografering. De oprindelige lovforarbejder angav, at det kunne virke krænkende for personer at blive fotograferet i situationer, hvor de var uforberedte. Frygten var, at der ville blive skabt en almindelig fornemmelse

[152] Det Kriminalpræventive Råds høringssvar af 8. januar 2020.
[153] Brottsförebyggande rådet (BRÅ) (2018): CCTV and Crime Prevention. Systematisk Review udgivet i samarbejde med University of Cambridge.
[154] Med strenge krav til forsøgenes videnskabelige kvalitet og opsætning med kontrolgrupper, randomiseret udvælgelse og fokus på statistisk signifikans.
[155] Se mere om hvorvidt tv-overvågning kan forebygge kriminalitet på rådets hjemmeside: https://dkr.dk/flere-/trygge-byer/fakta-om-tv-overvaagning.
[156] Ved lov nr. 278 af 9. juni 1982 om forbud mod privates tv-overvågning mv.
[157] L151 af 12. marts 1982. FT 1981/82, tillæg A, sp. 3831f.

af ufrihed, hvis udbredelsen af overvågningsudstyr førte til, at folk, når de færdedes frit tilgængelige steder, ville føle sig udsat for at blive iagttaget af ikke tilstedeværende personer.[158]

Tilsynsmyndigheden på området, Datatilsynet, udtrykte gennem sin praksis efter persondataloven (gældende fra 2000 – 2018) det grundlæggende synspunkt, at offentlige myndigheder ud fra proportionalitetsbetragtninger normalt skulle undlade at videoovervåge de områder, som var opregnet i lovens § 1, stk. 1, nemlig gade, vej, plads eller lignende område, som benyttes til almindelig færdsel. [159] Det fælles europæiske databeskyttelsesorgan [160] gjorde det lidt mere vidtgående synspunkt gældende, at før overvågning overhovedet kunne anvendes, skulle mindre indgribende midler tydeligt have vist deres utilstrækkelighed og/eller uegnethed i forhold til specificerede og legitime formål med videoovervågningen.[161]

Adgangen til videoovervågning efter tv-overvågningsloven er imidlertid løbende blevet udvidet og allerede i 2007 fandtes loven mere at tage sigte på at regulere, hvor og hvordan videoovervågning kunne ske. [162] Tv-overvågningslovens titel blev derfor ændret således, at ordene "forbud mod" helt udgik, selvom det generelle forbud mod privates videoovervågning af gade, vej, plads eller lignende område, som benyttes til almindelig færdsel, stadig var udgangspunktet.[163]

I 2007 blev antallet af private aktører, der kan foretage videoovervågning, udvidet.[164] I 2010 og 2011 blev boligselskabers, idrætsanlægsejeres og kommuners adgang til tv-overvågning yderligere udvidet.[165] Udvidelsen blev begrundet af hensyn til kriminalitetsbekæmpelse i udsatte boligområder og for boligselskaber og idrætsanlægsejere tillige af hensyn til kriminalitetsbekæmpelse omkring idrætsanlæg.[166] Videoovervågning kunne i disse tilfælde tillades af politiet, hvis det var 'væsentligt' af hensyn til kriminalitetsbekæmpelse. Der kom herudover mulighed for kommunalt tilskud til privat tv-overvågning i 2016,[167] samt øgede muligheder for at dele videoovervågningsmateriale mellem erhvervsdrivende i 2018.[168]

6.3.2 Markant udvidelse af tv-overvågningsloven i 2020

I 2020 blev der gennemført markante udvidelser af adgangen til videoovervågning, idet der bl.a. i meget væsentlig grad blev ændret ved afstandskravet, som handler om, hvor langt videoovervågningen må brede sig i forhold til det egentlige mål for overvågningen. Det kan f.eks.

---

[158] Lind, Motzfeldt og Tranberg: TV-overvågning anno 2008 Erhvervsjuridisk Tidsskrift 2008.64.
[159] Lind, Motzfeldt og Tranberg: TV-overvågning anno 2008 Erhvervsjuridisk Tidsskrift 2008.64.
[160] Tidligere Artikel 29 gruppen, nu Det Europæiske databeskyttelsesråd, European Data Protection Board (EDPB).
[161] Lind, Motzfeldt og Tranberg: TV-overvågning anno 2008 Erhvervsjuridisk Tidsskrift 2008.64, afsnit 5.2.3.
[162] Se tv-overvågningsudvalgets betænkning nr. 1483/2006, bemærkninger til § 1, nr. 1.
[163] Jf. § 1, nr. 1 i lov nr. 519 af 6. juni 2007.
[164] Jf. § 1, nr. 2 i lov nr. 519 af 6. juni 2007.
[165] Jf. § 1, nr. 1 i lov nr. 713 af 25. juni 2010, og § 1, nr. 1 i lov nr. 422 af 10. maj 2011.
[166] Se lovforslag nr. 185 af 24. marts 2010, almindelige bemærkninger, pkt. 3.2.1 og 3.3.1. og lovforslag nr. 145 af 23. februar 2011, almindelige bemærkninger, pkt. 3.1.1.
[167] Jf. § 5, nr. 1 i lov nr. 1728 af 27. december 2016.
[168] Jf. § 1, nr. 2 i lov nr. 506 af 23. maj 2018.

være, at det lovlige formål er at overvåge en del af fortovet ved en pengeautomat, og så opstår spørgsmålet, hvor meget andet der også må overvåges for at opfylde formålet med overvågningen, som eksempelvis kan være at forebygge eller opklare kriminalitet i tilknytning til pengeautomaten.

Før 2020 var ordlyden af bestemmelsen, at hvis sådan overvågning fandtes at være klart nødvendig af hensyn til kriminalitetsbekæmpelse, kunne der overvåges områder i *direkte* tilknytning til facaden. I en dom fra 1998 fandt Vestre Landsret,[169] at overvågning i relation til indgangen til en klub, som strakte sig 100 m fra facaden, ikke kunne anses for at ligge i *direkte* tilknytning til facaden. Efter fast praksis fortolkedes afstandskravet som omkring 10-15 meter.

I 2020 blev ordlyden ændret således, at der nu kunne overvåges i *umiddelbar* tilknytning, hvilket i bemærkningerne blev tilkendegivet at udgøre op til 30 meter for både private og offentlige myndigheder.[170] Der skete også endnu en udvidelse af, hvilke private der kan foretage videoovervågning.[171] Samtidig blev der indført mulighed for, at alle private aktører (uden en nærmere afgrænsning af personkredsen) kan få tilladelse fra politiet til tv-overvågning, når den findes nødvendig for at imødegå en (ikke nærmere specificeret) sikkerhedstrussel.[172] Der blev ydermere indsat to brede bemyndigelsesbestemmelser for justitsministeren til at give tilladelse til mere privat og offentlig tv-overvågning, end hvad der allerede fulgte af loven.[173] For at lette politiets adgang til tv-overvågningsoptagelser i efterforskningsøjemed[174] blev det desuden gjort obligatorisk og forbundet med strafansvar for private aktører og offentlige myndigheder at registrere deres videoovervågning i politiets register over tv-overvågningskameraer (POLCAM).[175] Der blev herudover indført mulighed for at udvide opbevaring af videoovervågning optaget i kriminalitetsbekæmpende øjemed med henblik på stillingtagen til videregivelse. En adgang der i øvrigt er blevet udvidet løbende gennem årene.[176]

Det hører med til historien, at der i det først fremsatte lovforslag til 2020-ændringen oprindeligt var lagt op til en endnu lempeligere ramme for tv-overvågning, end den endeligt vedtagne. Der var bl.a. lagt op til at lempe nødvendighedskravet i forhold til, hvornår videoovervågning kan iværksættes, så videoovervågning ikke længere skulle være 'klart nødvendig' af hensyn til kriminalitetsbekæmpelse, men blot 'nødvendig'.[177] Det blev desuden foreslået at bevæge sig helt væk fra afstandskravet i forhold til, hvordan/hvor stort et område der kan tv-overvåges, og i stedet alene fokusere på en negativ afgrænsning om, at der ikke må tv-overvåges ind i private hjem eller andre private områder.

---

[169] UfR1998.1390V.
[170] Jf. §§ 1, nr. 5 og nr. 10 i lov nr. 802 af 9. juni 2020. Se også retsudvalgets betænkning nr. 102 af 19. maj 2020, ændringsforslag med bemærkninger, til § 1, nr. 1, § 1, nr. 3 og § 1, nr. 5 for nærmere specificering af afstandskravet.
[171] Jf. § 1, nr. 2 i lov nr. 802 af 9. juni 2020.
[172] Jf. § 1, nr. 7 i lov nr. 802 af 9. juni 2020.
[173] Jf. § 1, nr. 9, jf. § 1, nr. 6 og § 1, nr. 10 i lov nr. 802 af 9. juni 2020.
[174] Se lovforslag nr. 102 af 5. februar 2020, de specielle bemærkninger til § 1, nr. 10.
[175] Jf. § 1, nr. 10 i lov nr. 802 af 9. juni 2020.
[176] Jf. § 1, nr. 12 i lov nr. 802 af 9. juni 2020.
[177] Jf. § 1, nr. 5 og § 1, nr. 10 i lovforslag nr. 102 af 5. februar 2020. Se også de specielle bemærkninger til lovforslagets § 1, nr. 5, og § 1, nr. 10.

Dette forslag ville således i realiteten gøre op med forbuddet om at foretage bredspektret videoovervågning på offentligt sted. Formålet var et generelt hensyn til kriminalitetsbekæmpelse.[178]

Flere af de hørte myndigheder og organisationer var imidlertid stærkt kritiske over for denne udvidelse og slog bl.a. ned på den uklare sammenhæng og dermed manglende proportionalitet mellem udvidelsen af overvågningsområdet og formålet med overvågningen. Eksempelvis udtalte Advokatrådet, at "*med den foreslåede ændring af afstandskravet fra 30 til 100 m synes trygheden omkring den enkelte lokalitet (indgang, opgang mv.) ikke længere at være bærende for indsatsen. I stedet synes forslaget at være et middel til en bred, generel og i praksis ubegrænset adgang til borgerovervågning, hvor den enkelte lokation alene bliver et tilfældigt redskab hertil.*"[179]

Da der ikke på daværende tidspunkt var politisk opbakning til en så vidtgående adgang til videoovervågning, blev disse dele af lovforslaget ikke gennemført.

Lovændringen indeholdt derimod to bemyndigelsesbestemmelser til, at justitsministeren administrativt kunne fastsætte midlertidige regler om yderligere adgang for 1) privates adgang til at videoovervåge, hvis det fandtes 'nødvendigt' af hensyn til kriminalitetsbekæmpelse, og 2) kommuners adgang til at videoovervåge, hvis der fandtes 'behov for at fremme trygheden'[180]. Efter omfattende debat førte den parlamentariske proces til, at en sådan bekendtgørelse inden udstedelsen skulle i høring hos Folketingets Retsudvalg, som kunne forkaste udkastet. En bekendtgørelse kunne højst gælde i et år og kun forlænges ved ændring af loven. I forbindelse med lovændringen blev det endvidere tilkendegivet, at justitsministeren ville udarbejde en evaluering af den udvidede adgang til videoovervågning senest fire år efter 2020-ændringslovens ikrafttræden.[181]

6.3.3 Udvidelse af afstandskravet i 2024 og udskudt evaluering

Den i ovenstående afsnit beskrevne evaluering nåede ikke at blive gennemført, inden tv-overvågningsloven på ny blev ændret i juni 2024. Med ændringen i 2024 blev adgangen til videoovervågning igen øget markant. Som led i en politisk aftale med fokus på bekæmpelse af kriminelle bander,[182] blev der på ny foreslået og gennemført flere af de tidligere foreslåede meget vidtgående ændringer af tv-overvågningsloven. Lovændringen indebar bl.a. en forøgelse af afstandskravet fra 30 til 100 meter, idet ordet '"umiddelbar" blev fjernet fra det blot 4 år tidligere indførte kriterium om "umiddelbar tilknytning".[183] Dermed blev afstandskravet for både private

[178] Jf. §§ 1, nr. 5 og nr. 10 i lovforslag nr. 102 af 5. februar 2020. Se også de specielle bemærkninger til lovforslagets § 1, nr. 5, og § 1, nr. 10.
[179] Høringssvar af 9. januar 2020 fra Advokatrådet.
[180] Tv-overvågningslovens §§ 2, stk.6, jf. § 2, stk.1, nr. 5, og § 2c, stk. 3.
[181] Se Retsudvalgets betænkning nr. 102 af 19. maj 2020, ændringsforslag med bemærkninger, til § 1, nr. 1. Både Justitia og Institut for Menneskerettigheder havde anbefalet en sådan evaluering i deres høringssvar til det oprindelige lovforslag.
[182] November 2023: Aftale om bandepakke IV – Trygge nabolag i hele Danmark (justitsministeriet.dk), Se s. 6 og fokusområde 5: Flere og bedre værktøjer til myndighederne.
[183] Jf. § 6, nr. 1 i lov nr. 665 af 11. juni 2024. Se almindelige bemærkninger, pkt. 5.5. samt specielle bemærkninger til § 6, nr. 1 i lovforslag nr. 150 af 10. april 2024, for nærmere specificering af afstandskravet.

aktører og offentlige myndigheder udvidet ganske markant. I bemærkningerne til lovforslaget er følgende anført om baggrunden for, at det nu fandtes nødvendigt at overvåge op til 100 meter fra det, som har betinget overvågningen:

"Det er vurderingen, at det er nødvendigt at øge afstandskravet, da den udvidede adgang til tv-overvågning i visse situationer vil kunne være helt afgørende for, at politiet kan opklare kriminalitet. Når afstandskravet udvides, øges chancerne således også for, at kameraet fanger den begåede kriminalitet. Det bemærkes i øvrigt, at tv-overvågning også har et forebyggende sigte".[184]

Begrundelsen er en gentagelse fra det forkastede 2020-forslag,[185] og mange aktører var da også (igen) meget kritiske. Datatilsynet fandt det bl.a. yderst betænkeligt at lade private erhvervsdrivende og offentlige myndigheder udføre videoovervågning, som rækker ud over deres egne formål, og i stedet forfølger mere generelle politimæssige formål, som de pågældende kan have svært ved at vurdere lovligheden af. Der blev peget på både problemer i forhold til saglighed, proportionalitet og dataminimering, ligesom der helt generelt blev peget på, at udvidelsen øgede risikoen for konkrete og uproportionale indgreb i privatlivets fred, som f.eks. kortlægning af enkeltpersoners færden, og at det ville ramme et ganske betydeligt større antal personer uden nogen politimæssig interesse, end det tidligere har været tilfældet.[186] Datatilsynet pegede også på, at forslaget om et øget afstandskrav kunne skabe større usikkerhed i forhold til, hvor der rent faktisk videoovervåges, idet det kan være vanskeligt for borgere at vide, om man befinder sig på et videoovervåget areal i relation til den påkrævede skiltning, ligesom det kan være vanskeligt at vide, hvilken eller hvilke dataansvarlige der er ansvarlig for videoovervågning af det område, som man befinder sig på. Udover, at det skaber en øget risiko for misbrug, gør det det også meget vanskeligt for en borger i praksis at benytte sig af sine rettigheder til at gøre indsigelse mv.

Det Kriminalpræventive Råd var også kritisk og savnede en beskrivelse af formålet med den massive udvidelse. Der blev i den forbindelse bl.a. peget på, at der kun er en dokumenteret forebyggende effekt af videoovervågning i nogle helt bestemte situationer som f.eks. hærværk og indbrud i parkeringskældre, men ikke i relation til personfarlig kriminalitet, der var angivet som baggrunden for ændringerne.[187] Der blev herudover peget på, at også misbrugsrisici og sikkerhedsrisici øges i takt med omfanget af overvågningen og de mange yderligere oplysninger, som på denne måde ville blive opbevaret.

Det skal dog fremhæves, at flere af de meget vidtgående forslag fra 2020 ikke blev gentaget i 2024. De kvalificerede krav til nødvendighedsvurderingerne er bl.a. bibeholdt flere steder. Der er således fortsat krav om, at det for privates vedkommende skal være 'klart nødvendigt' [188] af hensyn til

[184] Se almindelige bemærkninger, pkt. 5.5. i lovforslag nr. 150 af 10. april 2024.
[185] Se de specielle bemærkninger til § 1, nr. 5, og § 1, nr. 10 i lovforslag nr. 102 af 5. februar 2020.
[186] Datatilsynets høringssvar af 7. marts 2024 (jnr. 2024-11-0084), afsnit 4.
[187] Høringssvar af 8. januar 2020. Det kriminalpræventive råd støtter sig bl.a. på en omfattende metaanalyse på området, udarbejdet af det svenske kriminalitetspræventive råd, BRÅ fra 2018.
[188] Tv-overvågningslovens §2, stk. 1, nr. 3, litra c.

kriminalitetsbekæmpelse, eller for boligforeninger og idrætsanlægsejer, hvis der foreligger et 'væsentligt hensyn' til kriminalitetsbekæmpelse.[189] Omvendt er der stadig adgang til at foretage videoovervågning for at 'fremme trygheden',[190] uden det er nærmere specificeret, hvad der ligger i dette begreb, ligesom der er bemyndigelse til, at der administrativt kan åbnes op for øget privat videoovervågning, hvis det vurderes 'nødvendigt af hensyn til kriminalitetsbekæmpelse'.[191]

I forbindelse med høringsprocessen anbefalede bl.a. andet Justitia, at man som minimum skulle lade den nye og markante udvidelse af adgangen til tv-overvågning afvente den lovede evaluering af udvidelserne i 2020-ændringsloven.[192] Evalueringen blev i stedet udsat 2 år med henblik på også at omfatte de nye udvidelser af adgangen til at overvåge, som blev vedtaget i juni 2024.[193]

6.4 Udviklingen i politiets overvågning med ANPG

I januar 2015 henvendte Rigspolitiet sig til Datatilsynet med henblik på at få en vejledende udtalelse om indførelse af en særlig type videoovervågningssystem som var integreret med en helt ny automatisk nummerpladegenkendelsesteknologi (ANPG). ANPG virker ved en automatisk aflæsning og registrering af nummerplader på alle biler, som passerer de steder, hvor der er placeret enten et ubemandet stationært ANPG-kamera eller et mobilt ANPG-kamera, som er monteret på et køretøj.[194] ANPG-systemet skulle behandle og opbevare fotos af køretøjet og oplysninger om nummerpladen, optagelsestidspunktet og køretøjets position på optagelsestidspunktet.[195]

Formålet med overvågningen var at indsamle og registrere oplysninger om køretøjer, som blev identificeret via genkendelse af nummerpladen, og på baggrund af automatisk søgning identificere biler af konkret interesse for politiet ud fra 'hotlister' med anførte nummerplader af interesse ud fra en række forskellige kategorier ('hits'). Derudover ønskede man også mere bredt at registrere 'no-hits' til efterforskningsmæssig brug i forhold til biler, som ikke i forvejen var vurderet politimæssigt interessante og derfor ikke fremgik af en hotliste. No-hits skulle opbevares i 30 dage svarende til rammerne i tv-overvågningsloven.

Rigspolitiet og Datatilsynet var enige om, at ANPG-systemet ville indebære indsamling, behandling og lagring af personoplysninger, da oplysningerne via registreringer om nummerpladen kunne henføres til personer. I henvendelsen til Datatilsynet oplyste Rigspolitiet desuden, at "*afhængigt af vinklen, lysforhold og kvaliteten af det enkelte foto vil det i nogle tilfælde være muligt at identificere*

[189] Tv-overvågningslovens §2, stk.3 og stk. 3.
[190] Tv-overvågningslovens § 2a, § 2b og i henhold til administrative regler efter §2c, stk. 3.
[191] Tv-overvågningslovens § 2, stk. 6, jf. stk.1, nr. 5.
[192] Se Justitias høringssvar af 12. marts 2024 til lovforslag om ændring af straffeloven, retsplejeloven og forskellige andre love (Gennemførelse af dele af Bandepakke IV).
[193] Se Justitsministeriets høringsnotat af 10. april 2024 om forslag til lov om ændring af straffeloven, retsplejeloven og forskellige andre love (Gennemførelse af dele af bandepakke IV).
[194] Jf. § 2 i bekendtgørelse nr. 1776 af 16. december 2015.
[195] Jf. § 3 i bekendtgørelse nr. 1776 af 16. december 2015.

fysiske personer i køretøjet".[196] Datatilsynet behandlede sagen på et møde i Datarådet og udtalte herefter, at den påtænkte behandling af personoplysninger med teknologien kun med visse begrænsninger kunne foretages indenfor rammerne af de dagældende regler i persondataloven, idet behandlingen gav anledning til overvejelser om foreneligheden med de grundlæggende principper for databeskyttelse.[197] Som eksempel tilkendegav Datatilsynet, at opbevaring af ***'no-hits'*** (nummerplader som ikke i forvejen var lagt ind i systemet af politimæssige grunde) *ikke* ville kunne anses for proportionelt eller sagligt, hvis de var indsamlet som led i almindelig patruljekørsel. Derimod kunne 'no-hits' indsamlet som led i en *målrettet indsats*, som f.eks. ved landegrænsen, opbevares i 30 dage.[198] For så vidt angår opbevaringen af '***hits'*** fandt Datatilsynet, at dette skulle begrænses til det konkret proportionelle for den enkelte kategori, ligesom kategorierne skulle være defineret ud fra præcise kriterier. Endelig fandt Datatilsynet, at retssikkerhedsmæssige hensyn tilsagde, at en regulering af systemets behandling af personoplysninger som minimum burde ske ved en bekendtgørelse.[199] Dette resulterede i den første bekendtgørelse om ANPG i december 2015,[200] som blev udstedt med hjemmel i den dagældende persondatalov.[201]

Ifølge bekendtgørelsen var der 13 kategorier af 'hits', som kunne opbevares i enten 3 måneder, 1 år eller 2 år afhængig af grovheden af den kriminalitet, som lå til grund for indsamlingen. 'No-hits' kunne opbevares i 30 dage, hvis de var indsamlet på baggrund af en *målrettet politiindsats, der var tidsmæssigt og geografisk afgrænset og iværksat på baggrund af en konkret politifaglig vurdering, hvor anvendelsen af ANPG vurderes at være af væsentlig betydning*.[202] 'No-hits' indsamlet som led i almindelig patruljering kunne af tekniske grunde opbevares i op til 24 timer med henblik på vurdering af, om der var tale om et 'hit', og de skulle herefter straks slettes.

I september 2017 blev ANPG-bekendtgørelsen udstedt igen med hjemmel i politiloven[203] og retshåndhævelsesloven.[204] I den forbindelse ændredes anvendelsesområdet til et noget bredere område svarende til politilovens § 2,[205] ligesom en række nye kategorier blev tilføjet hit-delen, dog overvejende af den type, som slettes efter 3 måneder.

---

[196] Se s. 6 i Justitsministeriets kommenterede oversigt over høringssvar om udkast til bekendtgørelse om politiets anvendelse af automatisk nummerpladegenkendelse (ANPG) af 2. december 2016.
[197] Datatilsynets udtalelse af 17. marts 2015 om brug af automatisk nummerpladegenkendelse. (j.nr. 2014-082-0114).
[198] Datatilsynets udtalelse af 17. marts 2015 om brug af automatisk nummerpladegenkendelse. (j.nr. 2014-082-0114).
[199] Datatilsynets udtalelse af 17. marts 2015 om brug af automatisk nummerpladegenkendelse. (j.nr. 2014-082-0114).
[200] Bkg. nr. 1776 af 16. december 2015 om politiets anvendelse af automatisk nummerpladegenkendelse (ANPG).
[201] Lov nr. 429 af 31. maj 2000 om behandling af personoplysninger.
[202] Jf. herved § 6 i bkg nr. 1776 af 16. december 2015.
[203] Jf. § 2 a, stk. 3, i lov om politiets virksomhed, jf. lovbekendtgørelse nr. 956 af 20. august 2015, som ændret ved lov nr. 671 af 8. juni 2017.
[204] Jf. § 14, stk. 2, og § 16, stk. 4, i lov nr. 410 af 27. april 2017 om retshåndhævende myndigheders behandling af personoplysninger.
[205] Politilovens § 2 er en meget bred gengivelse af politiets opgaveportefølje som - udover kriminalitetsbekæmpelse - også omfatter at yde andre myndigheder bistand, at afværge fare for forstyrrelse af den offentlige orden og at udføre andre opgaver, der følger af gældende ret eller i øvrigt har en naturlig tilknytning til politiet.

Der er tale om meget omfattende registreringer særligt for så vidt angår 'no-hit' oplysninger om nummerplader uden aktuel politimæssig interesse, som de registrerede i øvrigt er afskåret fra at få indsigt i. [206] Et tal oplyst af politiet i 2019[207] viser, at der i en periode på 30 dage var registreret 51.640.053 'no-hits' og 409.623 'hits'. Det svarer til, at 99,2% af alle oplysninger i ANPG er 'no-hits'. Overvågningen er i en analyse fra 2022 af lektor, PhD Tanja Kammersgaard Christensen fra Aalborg Universitet vurderet som uforenelige med de grundlæggende rettigheder, hvilket navnlig baseres på en vurdering af de brede kriterier og uklare nødvendighed i forhold til de angivne formål med indgreb i privatlivets fred.[208]

I 2022 blev der på ganske markant vis skruet op for overvågningen med ANPG. Antallet af 'hit-kategorier' blev næsten fordoblet fra 13 til 22, som stort set alle først slettes efter den mellemlange slettefrist på 1 år, herunder f.eks. nummerplader tilknyttet personer, der er eftersøgt af humanitære grunde, til afsoning eller tilsigelse til et retsmøde[209].

Også overvågningen af 'no-hits' blev intensiveret, idet disse nu kunne indsamles ud fra et mindre konkret kriterium, *hvis det understøtter et eller flere strategiske indsatsområder i politiet, hvor anvendelsen af ANPG vurderes at være af væsentlig betydning*. Bekendtgørelsen stiller således ikke længere krav om en målrettet indsats, der er geografisk eller tidsmæssigt afgrænset og iværksat på baggrund af en konkret politifaglig vurdering.[210] Samtidigt blev opbevaringsperioden for 'no-hits' markant øget, så disse nu kunne opbevares i op til 60 dage.

Opbevaringsbegrænsningen vedrørende 'no-hits', som *ikke* er indsamlet som led i en målrettet indsats, men derimod indsamlet som led i almindelig patruljekørsel, blev samtidigt udvidet. Hvor de tidligere kun kunne opbevares i 24 timer af rent tekniske grunde, kunne de opbevares i op til 7 dage. Denne opbevaring ses ikke længere at være begrundet i tekniske hensyn, og det er uoplyst på hvilket grundlag, der nu er belæg for sådan behandling, som direkte strider mod Datatilsynets tilkendegivelser i udtalelsen fra 2015 om proportionalitet og saglighed. Det er uoplyst, i hvilket omfang Datatilsynet har forholdt sig til dette eller til proportionaliteten i de øvrige udvidelser. Datatilsynet tilkendegav i sin udtalelse vedrørende den påtænkte ændring alene, at udkastet til bekendtgørelse ikke gav anledning til bemærkninger.[211]

[206] Jf. § 12 i bkg. nr. 1080 af 20. september 2017 som ændret ved bkg. nr. 152 af 27. januar 2022.
[207] Se vedrørende aktindsigt til brug for artikel: Kammersgaard Christensen (2022). Automatisk Nummerpladegenkendelse – behandling af personoplysninger, proportionalitet og retten til privatlivets fred.
[208] Christensen, Tanja Kammersgaard. (2022). Automatisk Nummerpladegenkendelse – behandling af personoplysninger, proportionalitet og retten til privatlivets fred. Nordisk Tidsskrift for Kriminalvidenskab nr. 2/2022, s. 283: https://tidsskrift.dk/NTfK/article/view/132398
Institut for Menneskerettigheders høringssvar af 17. december 2021. I samme retning FDMs høringssvar af 13. december 2021.
[209] Jf. § 5, nr. 18 i bkg. nr. 1080 af 20. september 2017 som ændret ved bkg. nr. 152 af 27. januar 2022
[210] Jf. § 1, nr. 4 i bkg. nr. 152 af 27. januar 2022.
[211] Brev af 16. december 2021, j.nr. 2021-12-1083.

Intensiteten af ANPG-overvågningen er stigende. Ultimo 2024 forventes antallet af ANPG-kameraer at være øget fra 400 til 646, hvoraf langt de fleste vedrører stationære anlæg, som nu kan optage og gemme 'no-hits' i op til 60 dage. [212]

Oplysninger fra ANPG har siden 2017 også kunnet behandles i politiets tværgående analysedatabase, POL-INTEL, hvor de kan inddrages i tværgående informationsanalyser. Dette kan i praksis betyde, at oplysningerne underlægges nye og væsentligt længere slettefrister. [213]

6.5 Udviklingen i politiets tryghedsskabende videoovervågning

Siden 2018 er politiets videoovervågning på offentligt tilgængelige områder øget markant som led i en tryghedsskabende indsats. Med finansloven for 2018 blev politiet således tildelt midler til at øge brugen af videoovervågning i områder, hvor der er behov for en særlig tryghedsskabende indsats. I første omgang var midlerne øremærket til indkøb af 100 videokameraer og siden yderligere 50 kameraer.

I oktober 2019 lancerede den daværende S-regering udspillet "Tryghed og sikkerhed i det offentlige rum". Politiet fik i forlængelse heraf midler til etablering af yderligere 300 kameraer. Politiet har således med udgangspunkt i politiske aftaler etableret i alt 450 tryghedsskabende kameraer i perioden 2018-2023. [214]

Som nævnt i afsnit 6.1 kan politiet uden tilladelse fra domstolene selv beslutte at iværksætte observation i form af videoovervågning som led i en efterforskning, når overvågningen vedrører et frit tilgængeligt sted.[215] Grundlaget er en ulovbestemt proportionalitetsvurdering, og behandlingen af oplysninger skal ske indenfor rammerne af de generelle behandlingsprincipper i retshåndhævelsesloven.[216] Det er uafklaret, hvor konkret og alvorligt et efterforskningsmæssigt behov, der skal være tale om for at mere bredspektret overvågning som led i generel kriminalitetsbekæmpelse kan anses for proportionelt og foretages uden særskilt regulering. Der blev ikke, som ved videoovervågning med automatisk nummerpladegenkendelsesteknologi (ANPG), fastsat specifikke rammer for videoovervågningen.

De specifikke rammer for opsætningen af kameraerne findes således hverken i lov eller bekendtgørelse. I den politiske aftale om finansloven i 2018, fremgik det, at der var enighed om "*at øge brugen af videoovervågning i områder, hvor der er behov for en tryghedsskabende indsats*",

[212] Se Justitsministeriets besvarelse af spørgsmål nr. 817 (Alm. del) fra Folketingets Udvalg af 18. april 2024.
[213] Se hertil bekendtgørelse nr. 1078 af 20. september 2017 om politiets behandling af oplysninger i forbindelse med tværgående informationsanalyser (POL-INTEL) samt kritisk i forhold til forenelighed med de grundlæggende rettigheder Kammersgaard Christensen (2024): POL-INTEL - er politiets behandling af personoplysninger i overensstemmelse med EU's retshåndhævelsesdirektiv? Nordisk Tidsskrift for Kriminalvidenskab nr.2 /2024.
[214] Se besvarelse af spm. 816 af 21. marts 2024 fra Folketingets Retsudvalg.
[215] UfR 2021.1262.
[216] Lov nr. 410 af 27. april 2017 om retshåndhævende myndigheders behandling af personoplysninger, som regulerer politiets behandlinger af personoplysninger med henblik på at forebygge, efterforske, afsløre eller retsforfølge strafbare handlinger mv.

samt at kameraerne skulle opsættes på "*lokationer, hvor der erfaringsmæssigt jævnligt opstår episoder med vold og uro. Det vil særligt være lokationer, som er præget af verserende bandekonflikter eller lignende.*"[217] Konteksten indebar, at videoovervågningen meget hurtigt skulle sættes i værk.

Af det efterfølgende politiske udspil fra 2019 - 'Tryghed og Sikkerhed i det offentlige rum' - fremgik det, at "*Regeringen vil afsætte midler til, at politiet kan opsætte 300 yderligere kameraer med henblik på både at forebygge og efterforske kriminalitet. Politiet vil på baggrund af en politifaglig vurdering udvælge de steder, hvor der er størst politimæssigt behov for at etablere tv-overvågning.*"[218]

Af politiets hjemmeside fremgår,[219] at kameraerne er placeret på baggrund af politikredsenes egne politifaglige vurderinger, og at dette betyder, "*at de kommer til at hænge på steder, hvor der på grund af kriminalitet eller utryghedsskabende kriminalitet er et særligt behov*".

I 2021 offentliggjorde Rigsrevisionen en beretning med en undersøgelse af, om politiet havde placeret overvågningskameraerne, så de havde størst mulig effekt på bekæmpelsen af utryghedsskabende gadekriminalitet. [220] Rigsrevisionen konkluderede bl.a., at politiet ikke vurderedes at have sikret sig, at de havde tilstrækkelig viden til rådighed forud for udvælgelsen af konkrete kameralokationer.[221] Derudover fandt Rigsrevisionen, at der var udvalgt mindst én lokation, som ikke levede op til Justitsministeriets krav om, at opsætningen af overvågningskameraer skulle ske på baggrund af en politifaglig vurdering. Rigspolitiet fandtes desuden ikke at have dokumenteret, hvorfor de valgte at opsætte kameraer, hvor de gjorde, og det var uklart, om der var udarbejdet en endelig vejledning, som politikredsene kunne tage udgangspunkt i ved opsætning af kameraerne.[222]

Rigsrevisionens undersøgelse vedrørte først og fremmest en vurdering af, om Rigspolitiets proces for fordeling af kameraerne i forhold til de udpegede lokationer for placering havde givet den størst mulige effekt i forhold til overvågningens formål. Justitsministeriet var ikke enig i Rigsrevisionens metode for effektmåling, som var baseret på Rigsrevisionens egen forståelse af formålet med overvågningen ud fra det, som fremgik af de politiske aftaler om baggrunden for de tildelte midler. Om grundlaget for selve placeringen af kameraerne blev det i ministerens redegørelse med svar på Rigsrevisionens kritik anført,[223] at politiets opsætning af overvågningskameraer ikke alene skulle vurderes ud fra, om kameraerne var placeret, hvor der er mest gadekriminalitet og at kameraerne var et vigtigt værktøj mod utryghed. Det fremgik, at kameraerne skulle opsættes på steder som led i den

[217] Politisk aftale om finansloven 2018, s. 26. https://www.regeringen.dk/media/4500/aftale-om-finansloven-for-2018.pdf.
[218] 'Tryghed og Sikkerhed i det offentlige rum' (2019), afsnit 4 'Politiet styrker brugen af videoovervågning'. https://www.regeringen.dk/media/7435/tryghed-og-sikkerhed-i-det-offentlige-rum.pdf.
[219] https://politi.dk/rigspolitiet/nyhedsliste/50-nye-kameraer-paa-vej-i-landets-politikredse/2020/08/19.
[220] Rigsrevisionens beretning af 21. oktober 2021 om politiets patruljering og overvågningskameraer: https://www.rigsrevisionen.dk/Media/637698949985101606/SR0221.pdf.
[221] Rigsrevisionens beretning af 21. oktober 2021 om politiets patruljering og overvågningskameraer, delkonklusion s. 30.
[222] Rigsrevisionens beretning af 21. oktober 2021 om politiets patruljering og overvågningskameraer, s. 45.
[223] Justitsministeriets notat af 20. december 2021 med ministerredegørelse til statsrevisorerne, afsnit 3.1. https://www.rigsrevisionen.dk/Media/637774926797293629/2-2021-JM.pdf.

særlige tryghedsskabende indsats, som var en væsentlig del af det politisk fastsatte mål i forbindelse med de bevilgede midler til placeringen og opsætningen af kameraerne.

Det er uoplyst, om Datatilsynet har været inddraget i forbindelse med stillingtagen til en eventuel regulering af politiets brug af tryghedsskabende kameraer. Det er muligt, at tilsynet ikke – som det ellers var tilfældet med ANPG – blev inddraget, inden beslutning om øget overvågning af tryghedsskabende grunde i det offentlige rum blev truffet. I forlængelse heraf bemærkes, at Datatilsynet – efter det politisk var besluttet i sommeren 2024 at lade politiet anvende ansigtsgenkendelsesteknologi uden retskendelse – af egen drift fandt anledning til at stille spørgsmål til Rigspolitiet om deres overvejelser i forhold til de databeskyttelsesretlige krav til brugen af ansigtsgenkendelsesteknologien.[224] Dette kunne tyde på, at Datatilsynet heller ikke i forbindelse med overvejelserne om brug af ansigtsgenkendelsesteknologi er blevet inddraget inden beslutning om anskaffelse blev truffet.

6.6 Delkonklusion

Videoovervågning på offentligt tilgængeligt sted er gennem mange år blevet anvendt som led i kriminalitetsbekæmpelsen i Danmark, fordi det kan være et effektivt efterforskningsmæssigt værktøj. I dansk ret er det traditionelt blevet betragtet som krænkende, hvis en udbredt anvendelse af overvågningsudstyr begrænser mulighederne for at kunne færdes på frit tilgængelige områder uden at blive udsat for skjult iagttagelse eller fotografering.[225] EU-domstolen har ligeledes lagt til grund, at der er tale om et indgreb i retten til privatliv og beskyttelse af personoplysninger.[226]

Som nævnt i afsnit 3.2.1 er retten til privatliv ikke en absolut ret. Efter fast praksis fra både Menneskerettighedsdomstolen og EU-domstolen kan staten gøre indgreb i grundlæggende rettigheder, hvis indgrebet skal forfølge et legitimt formål, indgrebet har en klar lovhjemmel, og indgrebet kan anses for at være nødvendigt og proportionalt i et demokratisk samfund. Ved særligt *intensive* indgreb *skærpes* kravene til, hvornår de enkelte betingelser kan anses for opfyldt.

Staten har samtidig pligt til at sikre, at behandlingen af borgernes oplysninger sker til udtrykkeligt angivne saglige formål samt på en rimelig og gennemsigtig måde, jf. herved den særlige beskyttelse af behandlingen af personoplysninger i EU's charters artikel 8.

EU-domstolen har i sin praksis slået fast, at videoovervågning med henblik på kriminalitetsbekæmpelse kan udgøre et **legitimt formål,** *hvis* videoovervågningen både er aktuel og effektiv, og ikke har 'hypotetisk karakter' i forhold til formålet.[227] De seneste udvidelser af

[224] Se Datatilsynets høring til Rigspolitiet med spørgsmål til politiets overvejelser ift. reglerne om databeskyttelse, herunder om risikovurdering og konsekvensanalyse med udgangspunkt i de registreredes rettigheder: https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2024/sep/datatilsynet-stiller-spoergsmaal-til-rigspolitiet-om-ansigtsgenkendelse.
[225] L151 af 12. marts 1982. FT 1981/82, tillæg A, sp. 3831f samt rapportens afsnit 6.1.
[226] EUD af 11. december 2019, Case of TK (C-708/18). Se også rapportens afsnit 3.2.3.
[227] EUD af 11. december 2019, Case of TK (C-708/18), præmis 44-47.

videoovervågning i henhold til tv-overvågningsloven, hvor kommuner i visse situationer kan videoovervåge ved behov for at fremme trygheden, samt overvågning som led i politiets tryghedsskabende indsats kan give anledning til alvorlig tvivl, om hvorvidt denne legitimitetsbetingelse er opfyldt. Når justitsministeren overfor statsrevisorerne har tilkendegivet,[228] at overvågningen ikke nødvendigvis skal sættes op, hvor der er mest gadekriminalitet, og overvågningen heller ikke kan anses at have et *forebyggende* sigte i relation til personfarlig kriminalitet, der var angivet som formålet med videoovervågningen, må det give anledning til betydelig tvivl om, hvad der er det legitime formål med overvågningen. Da overvågningen samtidigt er økonomisk prioriteret og nu omfatter mindst 450 kameraer, er der tilmed tale om en intensiv overvågning i det offentlige rum, der omfatter mange mennesker, som ikke på nogen måde mistænkes for at have begået kriminalitet.

Indgreb i privatlivsbeskyttelsen stiller som nævnt også særlige krav til **retsgrundlagets klarhed og kvalitet.** Også i forhold til denne betingelse giver politiets tryghedsskabende overvågning anledning til alvorlig tvivl. Efter menneskerettighedsdomstolens praksis indebærer kravet nemlig, at det ud fra retsgrundlaget skal stå klart, *hvem* der er omfattet af overvågningen, og *hvilke formål* overvågningen tjener. Det skal så at sige være muligt at forudse sin retsstilling (hensynet til gennemsigtighed og *foreseeability*).[229] "Tryghedsskabelse" er imidlertid ikke nævnt i retshåndhævelsesloven som et lovligt behandlingsformål for politiet.[230] Overvågningen ses alene reguleret i det politiske udspil og en ulovbestemt proportionalitetsgrundsætning. Retsgrundlaget var tilsyneladende så uklart, at Rigsrevisionen ved deres effektmåling i 2021 – på trods deres grundige undersøgelse - ifølge justitsministeren tog fejl af kriterierne for opsætningen af kameraerne.[231]

Også på *ANPG-området* giver de nu endnu mindre præcise kriterier for indsamling og opbevaring af 'no-hits' anledning til at stille spørgsmål ved, om betingelsen om klart retsgrundlag er opfyldt. Intensiteten af indgrebet skal også ses i lyset af, at der samtidig sættes mange flere kameraer op, og at der derfor også i praksis vil blive indsamlet væsentlig flere oplysninger fremadrettet, som tillige vil blive opbevaret i længere tid. Oplysninger, som vedrører billeder af biler og nummerplader *uden* aktuel politimæssig interesse, vedrørte i henhold til en opgørelse fra 2019 over 51 mio. biler i en 30 dages periode og udgjorde over 99 pct., af alle indsamlede oplysninger via ANPG.[232] Et antal og en andel der også kan give anledning til tvivl om selve *legitimiteten* af overvågningen i kraft af den nærmeste hypotetiske karakter af overvågningen, hvor kun en forsvindende lille andel af oplysningerne har eller vil få reel relevans i kriminalitetsopklarende øjemed.

---

[228] Justitsministeriets notat af 20. december 2021 med ministerredegørelse til statsrevisorerne, afsnit 3.1.
[229] Se rapportens afsnit 3.2 om bl.a. EMD af 4. maj 2000, Rotaru vs. Rumænien, og EMD af 29 June 2006, Weber and Saravia
[230] Retshåndhævelseslovens § 9, nævner kun forebygge, efterforske, afsløre, retsforfølge strafbare handlinger eller fuldbyrde strafferetlige sanktioner.
[231] Rigsrevisionens beretning af 21. oktober 2021 om politiets patruljering og overvågningskameraer, samt Justitsministeriets notat af 20. december 2021 med ministerredegørelse til statsrevisorerne, afsnit 3.1.
[232] Kammersgaard Christensen (2022). Automatisk Nummerpladegenkendelse mv.

Nødvendighed og proportionalitet er den tredje betingelse som skal være opfyldt for, at et indgreb i privatlivet kan være berettiget. Efter fast praksis må indgrebet ikke gå videre end det, som er det *strengt nødvendige,* og indgrebet skal konkret være *proportionelt* i forhold til det *legitime* formål, som ønskes opnået. Der ligger også heri, at et uklart legitimt formål vil få indflydelse på proportionalitetsafvejningen, idet kravene til *nødvendigheden* af overvågningen i så fald skærpes, ligesom tilfældet er for særligt intensive indgreb, hvor f.eks. mange borgere er omfattet, og det er en særligt beskyttelsesværdig aktivitet, der overvåges. [233] Ved videoovervågning indebærer nødvendighedsbetingelsen bl.a. en vurdering af, om overvågningens formål kan tilgodeses ved andre, mindre indgribende midler, herunder om det er tilstrækkeligt at overvåge i et mere afgrænset tidsrum eller område.[234]

Inden for alle tre videoovervågningsområder kan der efter Justitias opfattelse rejses tvivl om, hvorvidt nødvendighedsbetingelsen er tilstrækkeligt tilgodeset i retsgrundlaget.

Det gælder bl.a. for videoovervågning efter *tv-overvågningsloven*, hvor markante udvidelser af afstandskravet har udvidet private aktørers skøn ganske betragteligt i forhold til, hvor stort et område videoovervågning er nødvendig for. Dertil kommer, at den kriminalitet, som overvågningen er målrettet, ikke er nærmere specificeret, men kan være af mere generel karakter og dermed foretages ud fra en politimæssig/samfundsmæssig interesse, og således ikke længere er knyttet til den private aktørs egne interesser.

For *politiets nummerpladeovervågning (ANPG)* gælder det den markant øgede adgang til både at indsamle og efterfølgende opbevare 'no-hits', hvor millioner af billeder af biler og nummerplader uden aktuel politimæssig nu kan opbevares i op til 60 dage til efterfølgende politimæssig brug i en endnu ukendt efterforskningsmæssig sammenhæng. Dertil kommer, at politiet nu også indsamler 'no-hits' ved almindelig, ikke målrettet patruljekørsel, som opbevares i 7 dage. En behandling som Datatilsynet tidligere har tilkendegivet ikke kunne anses for hverken saglig eller proportional. [235]

I forhold til den *tryghedsskabende overvågning* er en proportionalitetsafvejning i realiteten umulig, fordi det angivne formål - tryghedsskabende - ikke er klart defineret i retsgrundlaget. Det får betydning for alle tre indgrebsbetingelser, som ikke kan anses for opfyldt i forhold til denne type overvågning. Det er endvidere uoplyst, i hvilket omfang der skal tages stilling til, om mindre indgribende midler kunne være anvendt, eller til overvågningens tidsmæssige eller geografiske udstrækning på de enkelte lokationer.

[233] EUD af 11. december 2019, Case of TK (C-708/18), pr. 44-47.
[234] EUD af 11. december 2019, Case of TK (C-708/18), pr. 44-47 samt EMD af 4. maj 2000, Rotaru vs. Rumænien, pr. 50- 52, og EU-domstolens afgørelse af 8. april 2014 (Forenede sager C-239/12 og C-594/12) Digital Rights. Se også rapportens afsnit 3.2.4 EDPB om særlige begrænsninger på områder knyttet til rekreative formål og fritidsaktiviteter.
[235] Datatilsynets udtalelse af 17. marts 2015 om brug af automatisk nummerpladegenkendelse.

Rigsrevisionens undersøgelse – hvor videoovervågningen i hvert fald i ét tilfælde ikke fandtes at være fastsat ud fra en konkret politifaglig vurdering – viser, at risikoen for at blive udsat for unødvendig videoovervågning må anses for reel.

Også de **databeskyttelsesretlige regler,** som har deres ophæng i EU's Charter om grundlæggende rettigheder, giver udfordringer i forhold til de tre videoovervågningsområder. Reglerne stiller krav om, at der kun indsamles oplysninger til udtrykkeligt angivne formål, at oplysninger ikke opbevares længere end nødvendigt, og at der med behandlingen i det hele taget sikres den fornødne grad af ansvarlighed (*accountability)* og gennemsigtighed i forhold til den, der foretager overvågningen.[236]

Når private og offentlige myndigheder kan videoovervåge store dele af offentligt tilgængelige områder ud fra et meget generelt kriminalitetsbekæmpende formål – som ikke er nært knyttet til det indgangsparti eller facade, som betingede overvågningen – har det indflydelse på både gennemsigtigheds- og ansvarlighedsprincippet. Formålet med overvågningen er ikke længere klart, eller noget de selv kan vurdere, og der kan stilles spørgsmål ved, hvem der i realiteten bliver ansvarlig for, at videoovervågningen sker lovligt.

Samlet set har staten med de seneste års udtrykkelige politiske intention om massivt at øge overvågningen i det offentlige rum bevæget sig meget langt væk fra den oprindelige og stærkt begrænsede adgang til videoovervågning i det offentlige rum, som byggede på hensynet til at kunne færdes på frit tilgængelige områder uden at blive udsat for skjult iagttagelse eller fotografering.[237] Det gælder både i forhold til de udvidede retlige rammer og for den markant øgede overvågningsintensitet, som skyldes forøgelsen af overvågningskameraer.

Med den stærkt øgede adgang til at videoovervåge og med ny potent ansigtsgenkendelsesteknologi på vej,[238] er der akut behov for en nærmere kortlægning og regulering, som kan sikre, at videoovervågning på frit tilgængeligt sted foretages ud fra *tilstrækkeligt legitime formål* og på et *tilstrækkeligt klart retsgrundlag,* der sikrer fokus på, at overvågning kun iværksættes de steder, hvor det er aktuelt og effektivt, og kun i det tidsmæssige og geografiske omfang, der er strengt nødvendigt for at opnå formålet. Disse elementer er afgørende for at sikre grundlæggende hensyn til rimelighed, gennemsigtig og ansvarlighed i forhold til beskyttelsen af borgernes ret til privatliv og beskyttelse af personoplysninger.

[236] Se ovenfor i afsnit 3.3 om Den Europæiske Menneskerettighedsdomstols praksis om krav til lovkvalitet.
[237] L151 af 12. marts 1982. FT 1981/82, tillæg A, sp. 3831f. Se også ovenfor i afsnit 4.3.1.
[238] Se Justitias rapport (2024) Ansigtsgenkendelsesteknologi – Behov for regulering af politiets anvendelse.

7 Dataovervågning

Kapitlet indledes i afsnit 7.1 med en redegørelse for udviklingen mod en mere og mere digitaliseret offentlig sektor i Danmark med omfattende datasamkøringer. Derefter gives der i afsnit 7.2 nogle eksempler på internationale erfaringer med digital kontrol, som har skabt retssikkerhedsmæssige udfordringer. I afsnit 7.3 og 7.4 sættes der fokus på den digitale kontrol, som udøves hos henholdsvis Udbetaling Danmark og Skat. Kapitlet afsluttes med en delkonklusion i afsnit 7.5.

7.1 Udvikling mod omfattende digitalisering og datasamkøring

Inden for de seneste 15 år er der sket en omfattende digitalisering af den offentlige sektor i Danmark. I perioden 2012-2015 vedtog Folketinget fire såkaldte bølgelove, der indførte digital selvbetjening på ikke mindre end 89 forskellige serviceområder. Siden da er endnu flere offentlige digitale selvbetjeningssystemer kommet til. Med Lov om Digital Post blev det siden den 1. november 2014 som udgangspunkt obligatorisk for alle borgere på 15 år og derover at modtage post fra det offentlige i digitale postkasser, og Danmark blev dermed det første land i verden, hvor digital selvbetjening i forhold til myndighederne er det klare udgangspunkt. Ikke overraskende er Danmark også i en længere årrække blevet kåret som både verdensmester og europamester i digitalisering.[239]

De offentlige digitaliseringsstrategier,[240] aftalen om digitaliseringsklar lovgivning i 2018 og aftalen mellem Regeringen, KL og Danske Regioner i 2020 om oprettelse en investeringsfond, der støtter afprøvning af nye teknologier i den offentlige sektor (de såkaldte signaturprojekter)[241] har alle bidraget til en accelererende udvikling henimod et kontinuerligt fokus på at høste fordelene af denne udvikling ved anvendelse af ny teknologi.

I takt med denne digitalisering, er der også blevet skabt grundlag for en væsentlig øget dataovervågning. Samtidig er Danmark et af de lande i verden, hvor datasamkøringer og digitale værktøjer bedst kan anvendes, idet danskerne siden 1968 med stor sikkerhed har kunnet identificeres entydigt på tværs af offentlige og private registre og databaser gennem personnummeret. Digitaliseringen har derfor betydet, at alle danskere er blevet markant mere overvågelige.

Det øgede fokus på effektivisering og besparelser i den offentlige sektor har været en drivende faktor for politiske prioriteringer i forhold til digitalisering af den offentlige sektor. Det har samtidig øget forventningerne til den tiltagende udnyttelse af tilgængelige data om borgerne, som er blevet øget i takt med udviklingen af nye analyseværktøjer og ny teknologi som machine-learning og kunstig intelligens.

---

[239] Se også Justitias rapport (2022) *Retssikkerhed for Digital Udsatte borgere*.
[240] Se om de sidste 25 års digitaliseringsstrategier: https://digst.dk/om-os/den-faellesoffentlige-digitaliseringsstrategi/25-aars-faelles-digitaliseringsstrategier/.
[241] https://digst.dk/kunstig-intelligens/signaturprojekter/ (187 mio. kr. på 40 projekter).

I Rigsrevisionen beretning fra 2015 [242] ses et eksempel på, hvordan den øgede digitalisering og samkøringsmuligheder i praksis stiller høje krav til effektiviteten af samarbejdet om kontrolindsatsen mellem Udbetaling Danmark og kommunerne. Rigsrevisionen stiller i undersøgelsen skarpt på både effektmåling og effektivisering af samarbejdet i forhold til kontrolindsatsen, som i vidt omfang baserer sig på samkøring af en række forskelligartede registre, deling af prioriteringslister mv.

I en velfærdsstat som den danske med en stor og skattefinansieret offentlig sektor er der et naturligt fokus på at sikre, at alle skatteborgere betaler deres skat. Det er samtidig nødvendigt med en vis form for kontrol, hvis man skal forhindre misbrug af offentlige ydelser. Det er et samfundsmæssigt problem og stødende for den kollektive retsfølelse, hvis borgerne ikke betaler deres skat eller får udbetalt ydelser, som de ikke er berettigede til. Det gælder naturligvis særligt, når der er tale om bevidst snyd.

Selvom der således er gode og legitime grunde til at føre kontrol med udbetaling af sociale ydelser og sikre en effektiv skattekontrol, må det forudsættes, at kontrollen udøves på en retssikkerhedsmæssig forsvarlig måde, og at kontrollen ikke udhuler borgernes fundamentale rettigheder, herunder borgernes ret til privatliv og beskyttelse af personoplysninger.

Samkøring af oplysninger i kontroløjemed og anvendelse af kompleks teknologi til effektivisering af kontrolindsatsen må desuden stille særlige krav til myndighederne i forhold til at sikre gennemsigtighed og ansvarlighed, så borgernes grundrettigheder ikke trædes under fode i jagten på effektivisering og kontrol med fejl og snyd.

Udviklingen på kontrolområdet har haft et stærkt fokus på myndighedsmæssig effektivitet, og den har muligvis i mindre grad tilgodeset grundlæggende hensyn til borgernes retssikkerhed og grundlæggende rettigheder. Datatilsynet gennemførte i 2023 en kortlægning af brugen af kunstig intelligens i den offentlige sektor, hvor det bl.a. kom frem, at langt de fleste projekter var iværksat *uden,* at der var foretaget de obligatoriske konsekvensanalyser, som har fokus på at sikre borgernes rettigheder i forbindelse med nye behandlingsformer. [243]

Særligt på to områder har der de seneste år været fokus på den myndighedsmæssige dataovervågning, der foretages gennem datasamkøring og anvendelse af ny teknologi. Det drejer sig om samlingen af en række opgaver vedrørende ydelsesudbetaling og kontrol hos Udbetaling Danmark og effektivisering af skattekontrollen. Dette er nærmere behandlet i afsnit 7.3 om Udbetaling Danmarks kontrolindsats mod fejl og snyd med sociale ydelser og i afsnit 7.4 om Skats kontrolindsats. I afsnit 7.2 nedenfor ses der først på retssikkerhedsmæssige erfaringer med digital kontrol og automatiserede processer.

[242] Rigsrevisionens beretning om samarbejdet mellem kommunerne og Udbetaling Danmark (2015).
[243] Datatilsynet (2023) Brug af kunstig intelligens i den offentlige sektor – kortlægning. Se også ovenfor i afsnit 4.1.3.

7.2 Internationale erfaringer med retssikkerhedsmæssige udfordringer

Digitaliseringen af den offentlige sektor i Danmark har skabt muligheder for øget effektivisering og besparelser, men udviklingen har samtidig skabt nye udfordringer for borgernes grundlæggende rettigheder og retssikkerhed. Øget datasamkøring og anvendelse af ny teknologi til kontrolindsatserne har betydet, at borgerne i højere grad bliver genstand for dataovervågning gennem profilering samt beslutningsunderstøttede og automatiserede afgørelser. Når teknologien anvendes uden tilstrækkelig opmærksomhed på, at den anvendte teknologi kan indeholde fejl eller bias, kan det imidlertid få alvorlige konsekvenser. Nedenstående eksempler understreger, hvor kritisk det kan blive, når myndighederne ikke balancerer ønsker om effektivisering gennem ny teknologi med fokus på og respekt for borgernes grundlæggende rettigheder.

Postmestre fejlagtigt anklaget for underslæb og bedrageri - Post Office Horizon skandalen

Post Office Horizon skandalen anses for en af de største retsskandaler i nyere britisk historie. Flere hundrede postmestre blev fejlagtigt anklaget for underslæb og bedrageri, da en softwarefejl i et it-system (Post Office Horizon) førte til forkerte registreringer. It-systemet, der blev indført i 1999, registrerede fejl, der blev tolket som økonomiske uregelmæssigheder. Det resulterede i, at mange postmestres regnskaber pludselig begyndte at give underskud. Et underskud, som postmestrene ikke kunne forklare, da de ikke havde indsigt i it-systemets automatiserede processer. Derfor valgte Post-Office at retsforfølge postmestre, når de ikke kunne forklare underskuddet. Mere end 700 postmestre blev retsforfulgt, hvor det for nogen endte med fængsling, økonomisk ruin og stigmatisering.[244]

The Post Office nægtede i årevis at anerkende problemerne med it-systemet og holdt fast i, at de fejl, som systemet rapporterede, skyldtes menneskeligt svigt. Først efter mange års kamp blev det afsløret, at det var it-systemet, som var problemet. I dag arbejder mange af de ramte på at få renset deres navn og har krævet erstatning for den uret, de har lidt.

Algoritme fratog familier børnetilskud - Børnepasningstilskudskandalen (kinderopvangtoeslagaffaire)

En af de mest opsigtsvækkende sager om myndigheders anvendelse af automatiserede systemer fandt sted i Nederlandene i perioden 2013-2019. Her blev tusindvis af familier fejlagtigt anklaget for socialt bedrageri og uretmæssige tvunget til at tilbagebetale sociale ydelser, på baggrund af en algoritmebaseret profilering, som vurderede borgere ud fra risikofaktorer om blandt andet nationalitet. Omkring 26.000 familier, primært personer med indvandrerbaggrund eller dobbelt statsborgerskab, blev anklaget for uretmæssigt at have modtaget tilskud og blev pålagt at tilbagebetale betydelige beløb.

Det viste sig efterfølgende, at algoritmen baserede sig på ufuldstændige og diskriminerende data, da den var ikke transparent, og der manglede menneskelig kontrol. De fejlagtige anklager var fortsat i årevis, uden de ansvarlige myndigheder greb ind. Først efter massiv kritik fra medier, eksperter og ofrene blev problemet afsløret. Skandalen førte i 2021 til, at premierminister Mark Rutte og hans kabinet trak sig fra deres poster.[245]

Automatiseret velfærdssystem udstedte uretmæssige krav om tilbagebetaling - Robodebt-skandalen

Et automatiseret velfærdssystem i Australien havde fra 2016 automatisk udstedt uretmæssige afgørelser med krav om tilbagebetaling af sociale ydelser. Systemet anvendte en algoritme, som sammenlignede indkomstdata fra skattemyndigheder med velfærdsregistre, hvilket resulterede i talrige fejlagtige påstande om overbetalinger. Hundredtusindvis af borgere modtog krav om tilbagebetaling uden menneskelig kontrol af afgørelserne

I 2019 erklærede domstolene systemet ulovligt. Den australske stat blev derefter pålagt at tilbagebetale 746 millioner australske dollars og afskrive gæld for yderligere 1,75 milliarder. En efterfølgende kommissionsundersøgelse bedømte projektet som et fundamentalt svigt i offentlig forvaltning.[246]

---

[244] BBC. Post Office Horizon scandal: Why hundreds were wrongly prosecuted. 30. juli 2024, https://www.bbc.com/news/business-56718036.

[245] Vice. How a Discriminatory Algorithm Wrongly Accused Thousands of Families of Fraud. 1. marts 2024.

[246] BBC. Robodebt: Illegal Australian welfare hunt drove people to despair. 7. juli 2023. https://www.bbc.com/news/world-australia-66130105.

7.3 Udbetaling Danmarks kontrolindsats

Udbetaling Danmark blev etableret i 2010[247] som en offentlig selvejende institution, der fra 2012 overtog en række af kommunernes sagsbehandlingsopgaver relateret til udbetaling af forskellige sociale ydelser. Et af målene med at samle sagsbehandlingen i én forvaltningsenhed var at effektivisere administrationen gennem stordriftsfordele.

Udbetaling Danmark har siden sin etablering fået tillagt stadig flere beføjelser og adgang til oplysninger på en række forskellige sagsområder i forbindelse med deres opgaver med bl.a. at bistå kommunernes kontrolindsats i forhold til fejl og snyd med sociale ydelser.[248] Justitia har både i 2015 [249] og 2019 [250] udgivet omfattende analyser af Udbetaling Danmarks systematiske dataovervågning, som omfatter adgang til at indhente og behandle oplysninger om borgerne uden deres samtykke eller nogen konkret anledning. Det gælder ikke kun i forhold til borgere, der ansøger om eller allerede modtager ydelser, men også deres samlevere, ægtefæller og andre husstandsmedlemmer samt deres formodede samlevere og husstandsmedlemmer. I konkret sag hos Datatilsynet, som Justitia fik aktindsigt i 2019, har Udbetaling Danmark oplyst, at de i praksis har behov for oplysninger om alle borgere i Danmark samt daglige opdateringer heraf for at kunne varetage sine myndighedsopgaver. Disse oplysninger tyder således på, at Udbetaling Danmarks behandling af personoplysninger reelt omfatter stort set hele Danmarks befolkning. I hvilket omfang der i praksis sker samkøring af oplysninger om alle disse borgere, afhænger dog af de kriterier, som løbende opsættes og udvikles for datasamkøringerne, herunder i hvilke tilfælde og omfang der tillige er behov for samkøring af oplysninger om ydelsesmodtagernes familie mv.[251]

Rapporter fra henholdsvis Justitia,[252] Institut for Menneskerettigheder[253] og Amnesty International[254] har peget på, at den meget omfattende indsamling, opbevaring, samkøring og videregivelse af oplysninger uden borgernes samtykke eller nogen konkret anledning, må anses for at være et indgreb, der er på kant med borgerens ret til privatliv og beskyttelse af personoplysninger.[255] Selvom

---

[247] Lov nr. 1594 fra 2010 (Etableringsloven).
[248] Lov 2012-04-11 nr. 324 om Udbetaling Danmark og lov 2015-04-29 nr. 523 om ændring af lov om Udbetaling Danmark med forarbejder.
[249] Justitia (2015): Udbetaling Danmark: En trussel mod privatlivets fred og retten til databeskyttelse.
[250] Justitia (2015): Udbetaling Danmark: En trussel mod privatlivets fred og retten til databeskyttelse.
[251] Se nærmere herom i Justitias rapport om Udbetaling Danmarks systematiske overvågning (2019), afsnit 5.4, s. 17-18.
[252] Justitia (2015): *Udbetaling Danmark: En trussel mod privatlivets fred og retten til databeskyttelse* og Justitia (2019): *Udbetaling Danmarks systematiske overvågning.*
[253] Institut for Menneskerettigheder: Forvaltningens kontrol, status 2015-2016.
[254] Amnesty International (2024): Coded Injustice: Surveillance and Discrimination in Denmark's automated welfare state.
[255] Jf. Den Europæiske Menneskerettighedskonvention med kommentarer af Peer Lorenzen m.fl., art. 1-9, 3. udg., s. 666. og 671-672, hvor det fremgår, at den systematiske indsamling og opbevaring af personoplysninger i offentlige myndigheders registre i sig selv kan være tilstrækkeligt til at aktualisere privatlivsbeskyttelsen og gøre EMRK artikel 8 anvendelig, og det samme gælder udveksling af personlige oplysninger mellem offentlige myndigheder uden samtykke fra den berørte person. Endvidere henvises til EU-domstolens dom i Digital Rights Ireland Ltd (sag C-293/12), hvor et EU-direktiv, som pålagde udbydere af offentligt tilgængelige elektroniske kommunikationstjenester og offentligt kommunikationsnet i et nærmere bestemt tidsrum at lagre trafik- og lokaliseringsdata i sig selv blev anset for at udgøre et indgreb i EU's Charter artikel 7 og 8, jf. præmis 34-37.

formålet med dataovervågningen er legitimt – at bekæmpe fejl og snyd med sociale ydelser – er Udbetaling Danmark beføjelser formuleret meget bredt, og det kan være vanskeligt fuldt ud at gennemskue konsekvenserne. F.eks. er mange af de oplysninger, som Udbetaling Danmark kan indhente og behandle, ikke nærmere defineret, ligesom der i vidt omfang ikke ses at være fastsat særlige begrænsninger for deres genanvendelse mv.[256]

Flere af de ovennævnte rapporter har også haft fokus på resultaterne af datasamkøringerne, og om metoden kan anses for at være et *nødvendigt* og *proportionalt* tiltag i forhold til det legitime kontrolformål, som søges opnået med kontrollen.

Justitias analyse fra 2019 viser, at Udbetaling Danmarks ugentlige datasamkøringer på egne områder i henholdsvis 2017 og 2018 omfattede op til 2,1 og 2,7 mio. ikke unikke ydelsesmodtagere. Hertil kom ydelsesmodtagernes familie og eventuelle øvrige husstandsmedlemmer, som der også blev samkørt oplysninger om.

Ud af de omfattende datasamkøringer blev der i 2017 overført 7.319 ydelsesmodtagere til en prioriteringsliste, som efterfølgende førte til oprettelse af 2.969 kontrolsager. Samme år var der 705 sager, som førte til standsning, ændring eller tilbagebetaling af ydelser på grund af fejl eller snyd. Der blev alene foretaget politianmeldelse i ca. 25 tilfælde.

I 2018 blev 4.081 ydelsesmodtagere overført til en prioriteringsliste, som førte til oprettelse af 2.325 kontrolsager. Samme år var der 1.094 sager, som førte til standsning, ændring eller tilbagebetaling af ydelser på grund af fejl eller snyd.[257]

I Amnesty Internationals nylige rapport fra 2024 er der også set nærmere på udbyttet af dataovervågningen. Analysens hovedfokus er de afledte retssikkerhedsmæssige spørgsmål i forhold til, om de anvendte algoritmer i praksis har en social slagside og derfor rammer skævt socialt og på en diskriminerende måde. Ifølge rapporten blev der i 2023 udbetalt ydelser til ca. 2,4 mio. modtagere og anvendt over 60 forskellige algoritmer baseret på AI og Machine Learning. På tre kontrolområder,[258] som bl.a. vedrører børne- og pensionsydelser samt ydelser i forbindelse med barsel, blev der udtaget i alt 1.414 sager af algoritmerne (undringslister). I samme år blev der endvidere udtaget 850 sager til nærmere kontrol inden for de samme kategorier og 123 sager endte med tilbagebetaling eller standset ydelse pga. snyd eller fejl. På grund af opgørelsesmetoden, er dette tal ikke nødvendigvis en delmængde af det udtagne tal på 1.414.[259]

Siden Justitias analyse i 2019 er lov om Udbetaling Danmark blevet ændret flere gange, og Udbetaling Danmark er blevet tillagt ansvar for administrationen af en række yderligere områder,

---

[256] Se Justitias analyse om Udbetaling Danmarks systematiske overvågning (2019) i afsnit 6.2.
[257] Justitia (2019): Udbetaling Danmarks systematiske overvågning, s. 10, 15-16 og 21.
[258] I analysen kaldes modellerne "really single", "model abroad" og "ficticious employment", se s. 44.
[259] Amnesty International (2024): Coded Injustice: Surveillance and Discrimination in Denmark's automated welfare state. s. 44. Tallene er opgjort i 2023, men alle sager er ikke nødvendigvis opstartet i 2023.
Se også: https://dm.dk/akademikerbladet/aktuelt/ai/2024/aktindsigt-masseovervaagning-af-danskere-faelder-36-pensionister/.

nye beføjelser og deraf følgende adgang til yderligere oplysninger. Det drejer sig bl.a. om opkrævning og tilbagebetaling af befordringsrabat for unge under uddannelse,[260] administration af ordning om skattefri seniorpræmie,[261] administration med midlertidige børnetilskud og tillæg til enlige forsørgere,[262] hjemmel til at indhente oplysninger om anciennitet i forbindelse med afgørelser om tidlig pension,[263] samkøring med henblik på kontrol af voldsdømtes modtagelse af social ydelser,[264] administration af ældrecheck og støtte til uddannelsessøgende med funktionsnedsættelse eller som er enlige forsørgere[265] samt administration vedrørende børnetilskud.[266]

Udviklingen er kun enkelte gange blevet mødt af grænser. Et eksempel på dette er et lovforslag fra 2018 om, at Udbetaling Danmark også skulle have adgang til oplysninger om borgernes el-forbrug, med henblik på at kunne efterprøve bopælspligt.[267] Forslaget blev imidlertid trukket tilbage efter omfattende kritik. Den daværende beskæftigelsesminister, Troels Lund Poulsen, udtalte efterfølgende, at "*indsatsen mod snyd med sociale ydelser ikke må betyde, at alle landets borgere skal overvåges*".

Justitia har også tidligere sat fokus på de retssikkerhedsmæssige konsekvenser af kommunernes kontrolindsats over for modtagere af sociale ydelser på baggrund af bl.a. resultaterne af Udbetaling Danmarks datasamkøringer. Justitias analyse viste, at kommunernes efterfølgende kontrol kan være både grænsesøgende og regeloverskridende, når der på grundlag af uklare og komplekse regler udføres omfattende fysisk observation af borgerne, kontrolbesøg i private hjem og overvågning af borgere via internettet.[268]

7.4 Skats kontrolindsats

Skattekontrollen er et andet område, hvor der i stigende omfang anvendes dataovervågning for at effektivisere kontrolindsatsen. Udviklingen de seneste år indeholder flere eksempler på, hvordan flere og flere oplysninger gøres tilgængelige for Skat til brug for bredspektret samkøring i kontroløjemed.

F.eks. indeholdt den tidligere gældende skattekontrollov frem til 2019 en bestemmelse, som gav told- og skatteforvaltningen adgang til at anmode offentlige myndigheder og private virksomheder om en lang række forskellige oplysninger, der af myndighederne skønnedes at være af væsentlig

[260] Lov nr. 1568 fra 2018, som trådte i kraft 1. juli 2019.
[261] Lov nr. 337 fra 2019, som trådte i kraft 1. juli 2019.
[262] Lov nr. 1550 fra 2019, som trådte i kraft den 1. januar 2020.
[263] Lov nr. 2202 fra 2020, som trådte i kraft 1. januar 2021.
[264] Lov nr. 452 fra 2022, som trådte i kraft 1. maj 2022.
[265] Lov nr. 455 fra 2023, som trådte i kraft 3. marts 2023.
[266] Lov nr. 266 fra 2024, som trådte i kraft 31. marts 2024.
[267] L98 / 2018-2019 LF.
[268] Justitia analyse (2019) *Kommunernes Kontrol med modtagere af sociale ydelser,* s. 16-29. https://justitia-int.org/analyse-kommunernes-kontrol-med-modtagere-af-sociale-ydelser/.

betydning for skatteligningen.[269] Skattemyndighederne var dermed tillagt et meget bredt skøn i forhold til, hvad der skønnedes nødvendigt.

I en analyse fra 2012 problematiserede CEPOS[270] Skats beføjelser, idet navnlig den brede skønsmargin fandtes at være i strid med menneskerettighedernes krav til et klart retsgrundlag, som yder tilstrækkelig beskyttelse mod vilkårlige indgreb.[271] Som eksempel på dette anførtes Skats praksis med at indhente teleoplysninger til brug for skatteligningen. Et sådant indgreb ville for politiet forudsætte en konkret mistanke om strafbart forhold af en vis grovhed samt kræve retskendelse, hvorfor det kunne anses for stærkt uproportionalt at lade Skat indhente denne type oplysninger på baggrund af et rent administrativt og bredt skøn.[272] Denne praksis blev genstand for en omfattende samfundsmæssig debat og blev efterfølgende standset i 2015 af den dagældende skatteminister.[273]

I forbindelse med en række lovpakker på skatteområdet blev Skats indhentningshjemmel ændret i 2019. I lovpakken 'Retssikkerhedspakke III – Klar og præcis lovgivning'[274] blev der indført en bestemmelse, som ændrede indhentningskriteriet fra 'væsentligt betydning' til alene at være *nødvendig,* hvilket indebar en udvidelse af rammerne for, hvilke oplysninger der kan indgå i skattekontrollen. Lovforslagets bemærkninger indeholdt en beskrivelse af den begrænsning i anvendelsen af teleoplysninger, som skatteministeren havde bekendtgjort i 2015, men begrænsningen fremgik ikke af selve lovteksten. Dette var bl.a. Justitia stærkt kritisk overfor, da det fandtes bedst stemmende med retssikkerhedsmæssige principper, at sådanne begrænsninger klart fremgår af retsgrundlaget.[275] Der blev efterfølgende stillet et ændringsforslag, hvor begrænsningerne blev indført i lovteksten med tydeliggørelse af grænserne for anvendelse af teleoplysninger i skattekontrollen.[276]

Ændringen af skattekontrolloven i 2019 gav også told- og skatteforvaltningen adgang til samkøring af it-systemerne til brug for myndighedsudøvelsen. Derudover blev der hjemlet terminaladgang til nødvendige oplysninger på tværs af forskellige registre både internt hos told og skattemyndighederne til brug for til brug for skatteansættelse og generel kontrol. Der blev ligeledes

[269] § 8D i lovbekendtgørelse nr. 1264 af 31. oktober 2013.
[270] Se analyse fra CEPOS v/ Jacob Mchangama fra 17. februar 2012 'Er SKATs beføjelser retsstridige?' Tilgængelig på: https://justitia-int.org/wp-content/uploads/2012/02/2012-02-22-Er-SKATs-bef%C3%B8jelser-retsstridige.pdf.
[271] CEPOS analyse s. 8 samt EMD af 5. december 2008, S and Marper vs. UK.
[272] CEPOS analyse s. 7.
[273] Skatteministeriets pressemeddelelse af 28. maj 2015: https://skm.dk/aktuelt/presse-nyheder/pressemeddelelsesarkiv/20150824-slut-med-teleoplysninger.
[274] L 2017-12-19 nr. 1535 som trådte i kraft 1.januar 2019 (lovforslag L13).
[275] Se også Justitias rapport af 20. marts 2017 om skats adgang til fortrolige teleoplysninger: https://justitia-int.org/wp-content/uploads/2017/02/Analyse_Ny-skattekontrollov-har-SKAT-stadig-adgang-til-fortrolige-teleoplysninger_20-03-17.pdf.
[276] Skatteudvalgets betænkning af 30. november 2017 til lovforslag nr. L13 om forslag til skattekontrollov.

til brug for opgørelse, opkrævning og inddrivelse af skatter, arbejdsmarkedsbidrag, told og afgifter givet hjemmel til terminaladgang til andre offentlige myndigheders registre med henblik på datasamkøring. [277]

I 2021 skete der yderligere udvidelser af adgangen til datasamkøring. Ved lovændringen blev skattemyndighedernes adgang til at indhente og samkøre en lang række oplysninger fra 'andre offentlige myndigheder' samt 'offentlige tilgængelige oplysninger' til brug for både skattekontrol og systemudvikling væsentligt udvidet. Lovændringen indeholdt en bred og ikke nærmere specificeret adgang til at indsamle og behandle *'alle nødvendige oplysninger om fysiske eller juridiske personers økonomiske og erhvervsmæssige forhold fra andre offentlige myndigheder og offentligt tilgængelige kilder, herunder samkøre sådanne oplysninger med de oplysninger told og skattemyndighederne måtte være i besiddelse af, med henblik på udvikling af it-systemer, der er nødvendige for skatteforvaltningens myndighedsudøvelse*'.[278]

Oplysningerne skulle bl.a. bruges til at udvikle en række risikoscoringsmodeller baseret på machine learning, som kunne bruges til at give skatteforvaltningen et bedre overblik og beslutningsgrundlag i forhold til at beslutte, hvilke borgere der med fordel kunne udtages til nærmere kontrol. [279] Lovændringen indeholdt endvidere en bemyndigelsesbestemmelse[280] om adgang til administrativt at fastsætte nærmere regler om samkøringen, herunder regler om hvornår og til hvilke formål der kan indsamles og behandles samt regler om opbevaringsperiode og sikkerhedsmæssige foranstaltninger.

Skatteministeriet vurderede, at ændringerne var af en sådan karakter, at de ville fravige det databeskyttelsesretlige grundprincip om formålsbegrænsning, [281] hvilket kun kan ske indenfor de snævre rammer for det *nationale råderum.*[282] Skatteministeriet anførte i den kommenterede høringsoversigt, at formålet udgjorde en nødvendig og forholdsmæssig foranstaltning i et demokratisk samfund af hensyn til bl.a. økonomiske og finansielle interesser.[283]

Ved lovændringen i 2021 blev der også lagt op til, at det i mere generelt omfang kunne undlades at orientere borgerne om indsamling af oplysninger om dem hos andre offentlige myndigheder og offentligt tilgængelige data.[284] Skatteforvaltningen anførte om grunden hertil, at det *"henset til den store datamængde"*, som skatteforvaltningen ville være i besiddelse af, og "*i takt med den generelle udvikling på området samt udviklingen af nye store it-systemer"* vurderedes at kræve en

[277] Skattekontrolloven § 38.
[278] Se om skattekontrollovens § 67a i L73 / 2021: https://www.ft.dk/samling/20211/lovforslag/L73/som_fremsat.htm.
[279] Se afsnit 2.1 i lovforslaget til L73.
[280] Skattekontrollovens § 67a, stk. 3
[281] Databeskyttelsesforordningens artikel 5, stk.1, nr. 2. Se herom ovenfor i afsnit 4.1. og 4.1.2.
[282] Se nærmere herom i afsnit 4.2.
[283] L73 / 2021, se bemærkninger til lovforslaget af 10. november 2021, afsnit 3.
[284] L73 / 2021, se bemærkninger til lovforslaget af 10. november 2021, afsnit 3.

uforholdsmæssig stor indsats at orientere borgerne i overensstemmelse med databeskyttelsesforordningens regler om oplysningspligt.[285]

Ved lovforslagets høring hos eksterne myndigheder og organisationer pegede Datatilsynet i sit høringssvar bl.a. på, at databeskyttelsesforordningen forudsætter, at det konkret vurderes, om oplysningspligt kan undlades. Datatilsynet fandt dog ikke anledning til at anfægte skattestyrelsens vurdering af, om det skulle betragtes som uforholdsmæssigt vanskeligt at foretage fornøden oplysning til de berørte borgere.[286] Datatilsynet forholdt sig overordnet forholdsvist neutralt til lovændringen ud fra en betragtning om, at det i sidste ende er en politisk beslutning, hvilke generelle samfundsinteresser, som findes at være tilstrækkeligt nødvendige og udgøre en forholdsmæssig foranstaltning i et demokratisk samfund, og dermed kan begrunde vedtagelse af regler, der vil fravige databeskyttelsesforordningen .[287]

Rækkevidden af de vedtagne ændringer blev efterfølgende problematiseret ved en eksperthøring i Folketinget flere måneder efter lovens vedtagelse. Ved denne høring blev der særligt sat fokus på foreneligheden med de grundlæggende rettigheder, proportionalitet og kravene til klare og præcise kriterier for overvågning af en sådan karakter.

7.5 Delkonklusion

Selvom der i en velfærdsstat som den danske med en stor og skattefinansieret offentlig sektor kan være gode grunde til at føre kontrol med f.eks. udbetaling af sociale ydelser og indbetaling af skat, må den meget omfattende databehandling, herunder samkøring af oplysninger, der finder sted som led i kontrolindsatsen hos både Udbetaling Danmark og Skat, og som sker uden at borgeren er informeret herom eller nogen konkret anledning, anses for at være et indgreb i borgerens ret til privatliv og beskyttelse af personoplysninger.

Som nævnt i afsnit 3.2.1 er retten til privatliv ikke en absolut ret. Efter fast praksis fra både Menneskerettighedsdomstolen og EU-domstolen kan staten gøre indgreb i grundlæggende rettigheder, hvis indgrebet skal forfølge et legitimt formål, indgrebet har en klar lovhjemmel, og indgrebet kan anses for at være nødvendigt og proportionalt i et demokratisk samfund.

Staten har samtidig pligt til at sikre, at behandlingen af borgernes oplysninger sker til udtrykkeligt angivne saglige formål samt på en rimelig og gennemsigtig måde, jf. herved den særlige beskyttelse af behandlingen af personoplysninger i EU's charters artikel 8.

Formålet med de indgreb i privatlivet, som foretages som led i kontrolindsatserne hos Udbetaling Danmark og Skat, er at bekæmpe fejl og snyd med henholdsvis sociale ydelser og skat. Det må i begge tilfælde anses for at være **legitime formål**.

[285] L73 / 2021, se bemærkninger til lovforslaget af 10. november 2021, afsnit 3, 2. spalte om opfyldelse af databeskyttelsesforordningens artikel 14.
[286] Datatilsynets høringssvar af 7. september 2021 (2021-11-0686).
[287] Datatilsynets høringssvar af 7. september 2021 (2021-11-0686).

Det er derimod mere tvivlsomt, om lovgrundlaget kan anses for at være af en sådan kvalitet, at de enkelte indgreb kan anses for tilstrækkelig afgrænsede og forudsigelige, samt om indgrebene er nødvendige og lever op til proportionalitetskravet.

I forlængelse heraf fremhæves det, at dataovervågning, der omfatter mange oplysninger om mange borgere, hvor det er muligt gennem samkøring på tværs af registre og sammenstilling med offentligt tilgængelige oplysninger at tegne en profil eller afdække bevægelsesmønstre må anses for at være særligt indgribende. Der må derfor stilles høje krav til **retsgrundlagets kvalitet**, så overvågningen gennemføres på en *gennemsigtig* og forudsigelig måde, og dermed sikrer den fornødne grad af ansvarlighed hos myndigheden.[288] Et klart retsgrundlag er et vigtigt retssikkerhedsmæssigt værn mod vilkårlighed i den myndighedsmæssige skønsudøvelse.

Derudover må der stilles krav til staten om, at denne type indgreb kun gennemføres, når det er strengt nødvendigt i demokratisk samfund og kun på en måde, som er proportionel i forhold til de formål, der søges forfulgt med overvågningen.

I takt med den øgede digitalisering og appetit på at anvende datasamkøring og datadrevne risiko-scoringsmodeller til at effektivisere og målrette kontrolindsatserne er der sket en gradvis udvanding af rammer for myndighedernes skøn. **Både Udbetaling Danmark og Skat har i deres retsgrundlag fået meget brede beføjelser** til selv at vurdere, hvilke oplysninger der er nødvendige for kontrolindsatsen. Det bliver derfor tiltagende uklart, hvor mange og hvilke oplysninger der indgår i datasamkøringerne, og hvilke øvrige myndigheder og private virksomheder, som oplysningerne indhentes fra.

Skats dataovervågning blev markant udvidet ved den i afsnit 7.4 nævnte lovændring fra 2021, hvorefter Skat kunne indhente '*alle nødvendige oplysninger* hos *offentlige myndigheder* og fra *offentligt tilgængelige kilder* uden nærmere specifikation af grænserne for, hvilke oplysninger, der kunne vurderes at være *nødvendige* for hverken skattekontrollen eller udviklingen af it-redskaber.

Udviklingen i Udbetaling Danmarks dataovervågning har særligt været kendetegnet ved en stadig voksende portefølje af kontrolopgaver med beføjelser til dataovervågning. Her behandles der oplysninger om stort set alle landets borgere, selvom antallet af borgere, der modtager de kontrollerede ydelser, er væsentligt lavere. I 2017 og 2018 var der ca. 2,4 mio. unikke ydelsesmodtagere.

Denne uklarhed i beføjelserne hos begge kontrolmyndigheder skaber risiko for vilkårlighed i myndighedsudøvelsen, og gør det vanskeligere som borger at forudsige sin retsstilling. Det kan derfor være i strid med betingelsen om et klart retsgrundlag.

[288] Se ovenfor i afsnit 3.3 om EMD's praksis om krav til lovkvalitet lovkvalitet, dvs. at lovgrundlaget skal være specifikt så det er muligt at forudse sin retsstilling (hensynet til gennemsigtighed og foreseeability), f.eks. EMD af 4. maj 2000, Rotaru vs. Rumænien, præmis 50- 52.

Dette underbygges bl.a. af processen i forbindelse med den i afsnit 7.4 omtalte lovændring på skattekontrolområdet fra 2021, og det politiske behov for at gennemføre en opklarende eksperthøring *efter* lovens vedtagelse, fordi rækkevidden af de nye kontrolbeføjelser blev anset for at være blevet for bred og uden et specifikt formål.

Dertil kommer hensynet til *gennemsigtighed* i forhold til borgerne. Gennemsigtighedshensynet kan komme under pres, når der behandles mange oplysninger om borgere inden for rammerne af et meget bredt myndighedsmæssigt skøn. Det gælder i særdeleshed også, når underretning af borgerne om databehandlingen kan undlades, fordi det vurderes at ville udgøre en stor ressourcemæssig belastning at orientere borgerne.

Uklarheden i retsgrundlaget gør det samtidig meget vanskeligt at forholde sig til **nødvendigheden af indgrebet** og dermed også **proportionaliteten**. Flere rapporter om Udbetaling Danmarks kontrolindsats [289] stiller spørgsmål ved, om udbyttet af kontrollen fuldt ud står mål med dataovervågningens omfang. På Udbetaling Danmarks område gælder det navnlig for de mange borgere, som ikke selv har ansøgt om sociale ydelser, men som løbende og uden samtykke indgår i den samlede dataovervågning.

Samlet set må den stigende anvendelse af teknologiske løsninger og algoritmer, som overvåger flere millioner borgeres data for at finde de fπå, anses for at indebære en betydelig risiko for at øge overvågningstrykket på flere måder, som ikke er forenelig med de grundlæggende rettigheder. Der er ovenfor påpeget en række alvorlige udfordringer ved både Udbetaling Danmarks og Skats kontrolindsats i forhold til menneskerettens betingelser for at gøre indgreb i borgernes ret til privatliv og beskyttelse af personoplysninger. Disse udfordringer må forventes at blive endnu større i fremtiden.

[289] Se ovenfor i afsnit 8 og 8.1. om Justitias analyse fra 2019 og Amnesty Internationals rapport fra 2024. Se også artikel i WIRED: How Denmark's Welfare State Became a Surveillance Nightmare | WIRED.

8 Konklusion

Den menneskeretlige beskyttelse af retten til privatliv og beskyttelse af personoplysninger indebærer, at staten kun kan gøre indgreb i disse rettigheder, hvis der foreligger et legitimt formål, et klart retsgrundlag og indgrebet findes nødvendigt og proportionalt i et demokratisk samfund. Staten har samtidig pligt til at sikre, at behandlingen af borgernes oplysninger sker til udtrykkeligt angivne saglige formål samt på en rimelig og gennemsigtig måde, jf. herved den særlige beskyttelse af behandling af personoplysninger i EU's charters artikel 8. Når det skal vurderes, om et myndighedsmæssigt tiltag rettet mod borgerne udgør et indgreb i individets grundlæggende rettigheder, spiller tiltagets *intensitet* også en afgørende rolle.

Digitaliseringen og den hastige teknologiske udvikling har for alvor påvirket appetitten for anvendelse af teknologi til overvågning og databehandling som led i effektivisering og kontrol. Udviklingen har fået en hastighed, der gør det særdeles vanskeligt at følge med i, hvilken intensitet eller overvågningstryk det enkelte tiltag medfører, ligesom det er blevet endnu vanskeligere at bevare overblikket over det samlede overvågningstryk.

Analyserne af de udvalgte retsområder i denne rapport vidner hver især om, at udviklingen i det samfundsmæssige overvågningstryk er præget af mange forhold, der hver for sig, men i høj grad også tilsammen giver grundlag for overvejelser i forhold til foreneligheden med de grundlæggende rettigheder og databeskyttelsesretlige principper.

Teknologiske muligheder inden for videoovervågning og dataovervågning anvendes i stigende omfang i Danmark til fuldt ud legitime formål som kriminalitetsbekæmpelse, kontrol af korrekt udbetaling af sociale ydelser og korrekt indbetaling af skat. Der opstår dog udfordringer med overholdelse af krav til retsgrundlagets klarhed, når myndighedernes skønsbeføjelser udvides for at sikre fleksible rammer til at høste de effektiviseringsgevinster, som teknologien sammen med den omfattende databehandling kan føre med sig. Et uklart retsgrundlag uden klare kriterier og rammer for det myndighedsmæssige skøn skaber risiko for, at myndighederne går for langt og ikke får taget fornøden stilling til, om de enkelte tiltag er strengt nødvendige eller kan nås med mindre indgribende midler. I nogle tilfælde kan overvågningens intensitet også nå et omfang, hvor der kan være grund til at stille spørgsmål ved legitimiteten, når mange borgeres oplysninger indsamles og behandles for at finde de få.

I et demokratisk samfund kan det sagtens være legitimt at skrue op for myndighedsbeføjelserne, men beskyttelsen af borgernes retssikkerhed og grundlæggende rettigheder er nødt til at følge med. De udgør selve grundstenen i en moderne, demokratisk retsstat. Derfor er det er også meget risikabelt at file på disse principper og rettigheder, uanset hvor gode de politiske hensigter er. Det kan hurtigt komme til at sætte tilliden til de offentlige myndigheder over styr, hvilket er yderst problematisk i en retsstat baseret på demokratiske værdier, hvor borgerne betragtes som frie og ligeværdige individer.

Tre faktorer med betydning for intensiteten af overvågningstrykket

Analyserne i denne rapport har afdækket en række faktorer, som hver for sig og tilsammen påvirker intensiteten af statens overvågning af borgerne. Overordnet kan faktorerne anskues fra tre vinkler: 1) Den teknologiske udvikling, 2) den politiske vilje og 3) de retlige rammer.

Den teknologiske udvikling har uden tvivl haft afgørende indflydelse på overvågningens intensitet og omfang. Det hænger sammen med, at ny teknologi øger sporbarheden og giver nye muligheder for at spore, sammenstille og profilere borgerne. Det muliggør en endnu mere intens, men ikke nødvendigvis mere ressourcekrævende overvågning og kontrol, da teknologien samtidig bliver billigere og mere tilgængelig.

Den politiske vilje er drivende for, i hvilket omfang den nye teknologi integreres i den kontrolorienterede myndighedsudøvelse. Påvirkningen af det øgede overvågningspres ses f.eks. tydeligt, når det politisk prioriteres at øge antallet af kameraer med henblik på øget overvågning i det offentlige rum. På dataovervågningsområdet har den politisk prioriterede digitalisering af den offentlige sektor, herunder den øgede behandling af oplysninger om borgerne i struktureret og søgbar form gennem apps og digital forvaltning, indebåret, at borgerne bliver mere overvågelige. Forventninger til myndighedsmæssig effektivitet har samtidig skabt øget incitament til at investere i nye it-systemer og teknologi som kunstig intelligens, der i endnu højere grad end tidligere kan intensivere overvågningen i bl.a. kontrolindsatserne. Den politiske vilje har samtidigt påvirket udvidelsen af *de* retlige rammer *for overvågning*, som ellers er det retssikkerhedsmæssige bolværk, der skal sikre, at den kontrolorienterede myndighedsmæssige overvågning ikke udhuler borgernes grundlæggende rettigheder.

Udviklingen af ***de retlige rammer*** er i særlig grad kendetegnet ved, at myndighedernes skøn i forhold til, hvornår der kan anvendes overvågning, er blevet stadig bredere. Dermed er det blevet mere uklart for borgerne, hvornår de kan blive udsat for overvågning.

Inden for *videoovervågning* er mulighederne for at overvåge for at 'fremme trygheden' eller af 'tryghedsskabende' grunde blevet markant udvidet, uden det er blevet nærmere defineret, hvad der ligger i dette udtryk, og uden at det kan dokumenteres at forebygge den kriminalitet, der gives som grund for overvågningen. Det rejser tvivl om legitimiteten af overvågningen. Samtidig bliver det meget vanskeligt at vurdere, hvornår en sådan overvågning er *nødvendig*, virksom og dermed *proportional*.

Når private og offentlige myndigheder kan videoovervåge store dele af offentligt tilgængelige områder ud fra hensyn til *generel kriminalitetsbekæmpelse* – og dermed ikke kun kriminalitet som er nært knyttet til det indgangsparti eller facade, som betinger overvågningen – har det også indflydelse på både gennemsigtigheds- og ansvarlighedsprincippet. Formålet med overvågningen er ikke længere klart, eller noget de selv kan vurdere, og der kan stilles spørgsmål ved, hvem der i realiteten bliver ansvarlig for, at videoovervågningen sker lovligt. Denne type ændringer i de retlige rammer kan indebære øget overvågning i det offentlige rum, som giver anledning til alvorlige

retssikkerhedsmæssige overvejelser både i forhold til det enkelte overvågningstiltag og i forhold til det samlede øgede overvågningstryk.

Inden for *dataovervågning* er rammerne for det myndighedsmæssige skøn til at vurdere, hvornår og hvilke oplysninger der systematisk skal videregives og samkøres i kontroløjemed, i væsentlig grad blevet udvandet. Myndighederne kan derfor mere eller mindre frit beslutte, hvad der kan anses for *nødvendigt* for kontrolindsatsen. Det indebærer en markant øget adgang til at indhente, genanvende og samkøre oplysninger både internt og med oplysninger indhentet fra andre myndigheder, private virksomheder og offentligt tilgængelige kilder. Det sker til formål, som både omfatter kontrol, profilering, risiko-scoring og til udvikling af algoritmer og it-systemer. Samtidig er der ikke nogen nærmere specifikation af, hvilke oplysninger det er nødvendigt at indhente, og det sker i vidt omfang også, uden borgerne orienteres. Overvågningen sker således hverken formelt eller reelt på en for borgerne *gennemsigtig* måde.

Sammenfattende indebærer den teknologiske udvikling, at personovervågningen og den deraf afledte myndighedsudøvelse hurtigt bliver meget intens og i accelererende grad kan øge overvågningstrykket på måder, som hverken var forudset eller forudsat i forbindelse med udvidelserne af de retlige rammer for overvågning.

Overvågningsområdet kalder først og fremmest på en meget større opmærksomhed på, at overvågning kun bør iværksættes på baggrund af regler, der efter en grundig lovgivningsproces og med rig mulighed for en samfundsmæssig debat udtrykkeligt tager stilling til formålene med databehandlingen og til, hvordan overvågning kan iværksættes på en måde, der sikrer rimelighed og gennemsigtighed for de borgere, som er genstand for overvågningen.

Derudover kalder området på en vedvarende og meget nøje afvejning af på den ene side teknologiske fremskridt og de muligheder, som teknologien og digitaliseringen indebærer, og på den anden side respekten for grundlæggende menneskerettigheder. Retsstatsprincipper og grundlæggende menneskerettigheder skal spille en langt større rolle, når nye eller udvidende overvågningstiltag overvejes. Det skal samtidig sikres, at sådanne beslutninger ikke tages alene ud fra vurderinger af det enkelte tiltag og dets ofte helt legitime og hæderværdige formål, men at det ses i sammenhæng med de mange andre tiltag, der allerede er iværksat, og som i vidt omfang tegner et stadig mere overvågeligt og overvåget samfund.

9 Anbefalinger

Anbefaling 1: Kommission for Privatlivets Fred

Overvågningstrykket i Danmark er vokset markant over de seneste årtier som følge af teknologiske fremskridt, øget datasamkøring og en udvidet brug af videoovervågning i det offentlige rum mv. Mange af disse tiltag er indført med henblik på at varetage vigtige samfundshensyn som kriminalitetsbekæmpelse og myndighedsmæssig effektivitet. Udviklingen udfordrer imidlertid i stigende grad borgernes grundlæggende ret til privatliv og beskyttelse af personoplysninger. Dette kan på sigt have en negativ effekt på borgernes grundlæggende tillid til offentlige myndigheder, hvilket er essentielt i en demokratisk retsstat.

Justitia anbefaler, at der nedsættes en Kommission for Privatlivets Fred, som skal vurdere rammer og generelle vilkår for beskyttelse af privatlivets fred i Danmark. Formålet er at sikre et solidt grundlag for en kvalificeret demokratisk debat om grænserne for statens indgreb i borgernes ret til privatliv og beskyttelse af personoplysninger. Kommissionen skal særligt have til opgave at vurdere, hvordan lovgivning og praksis kan balanceres, så varetagelse af nødvendige effektivitets-, kontrol- og sikkerhedshensyn ikke reelt udhuler borgernes ret til privatliv og beskyttelse af personoplysninger. Kommissionen skal også overveje, hvordan det kan sikres, at det samlede overvågningsomfang indgår i overvejelserne, når nye overvågningstiltag initieres og foreslås.

Anbefaling 2: Overblik over det samlede overvågningsomfang

De enkelte overvågningstiltag hver for sig, men i høj grad også tilsammen, udfordrer i stigende grad borgernes grundlæggende ret til privatliv og beskyttelse af personoplysninger. Der er derfor behov for et vedvarende fokus på ansvarlighed i forhold til både de enkelte overvågningstiltag og det samlede overvågningstryk, ligesom der er behov for at styrke mulighederne for et effektivt tilsyn med databehandlingen. Det er samtidig vigtigt, at både Folketinget, embedsværket og befolkningen har tilstrækkeligt indblik i overvågningstrykket.

Justitia anbefaler, at der udpeges en central instans, som løbende skal skabe overblik over myndighedernes samlede overvågning af borgerne, og i den forbindelse årligt skal udarbejde en offentlig tilgængelig redegørelse til Folketingets Retsudvalg om det samlede omfang af myndighedernes overvågning af borgerne. Derudover skal der indføres anmeldelsespligt til den centrale instans ved iværksættelse af nye overvågningstiltag.

Anbefaling 3: Klart retsgrundlag og sikring af demokratisk legitimation

Myndighedernes overvågning, der udgør indgreb i borgernes ret til privatliv og beskyttelse af personoplysninger, sker ofte på grundlag af uklare regler. Dette udfordrer ikke kun den demokratiske legitimitet, men også gennemsigtigheden for borgerne.

Justitia anbefaler, at alle fagministerier forpligtes til at sikre, at alle fremtidige og eksisterende overvågningstiltag beskrives og reguleres særskilt med et klart retsgrundlag med tydelig angivelse af de specifikke formål for overvågningstiltaget og i en form, som offentligheden kan få adgang til. Det gælder bl.a. på Beskæftigelsesministeriets område i forhold til Udbetaling Danmarks og på Skatteministeriets område i forhold til deres muligheder til at foretage dataovervågning i kontroløjemed. For så vidt angår politiets videoovervågning i det offentlige rum anbefales det, at Justitsministeriet tager initiativ til en mere generel undersøgelse af, om der er behov for en regulering af politiets observation og overvågning i det offentlige rum og på frit tilgængeligt område, herunder om politiets anvendelse af ansigtsgenkendelsesteknologi i forbindelse med videoovervågning skal reguleres som et straffeprocessuelt indgreb i retsplejeloven, der kræver retskendelse.[290] Herudover bør Justitsministeriet hurtigt tilvejebringe et klart retsgrundlag med entydige kriterier for, hvornår videoovervågning i det offentlige rum kan anses for tryghedsskabende.

Anbefaling 4: Grundig lovgivningsproces

Justitia har i en tidligere rapport (2024) *Udfordringer med Lovgivningsprocessen*, dokumenteret, at der i lovgivningsprocessen er udfordringer med at sikre en grundig parlamentarisk kontrol og samfundsmæssig debat om vidtgående overvågningsmæssige tiltag, herunder i forhold til anvendelsen af ny teknologi.

Justitia anbefaler, at alle lovforslag, som indeholder overvågningstiltag, ledsages af ensartede og strukturerede *konsekvensvurderinger* til belysning af retssikkerheds- og rettighedsmæssige konsekvenser, dataetiske overvejelser og en oversigt over allerede eksisterende overvågningstiltag på det pågældende område. Tilsvarende skal gælde ved behandling af bekendtgørelser om overvågningstiltag. Derudover anbefales det, at lovforslag om overvågningstiltag altid behandles i både Retsudvalget og det relevante fagudvalg. Denne proces kendes allerede fra den i 2018 indførte ordning vedrørende bekendtgørelser om dataovervågning i form af samkøring af oplysninger i kontroløjemed.[291]

Anbefaling 5: Overvågningsetisk reflektionsværktøj

Nye og effektive metoder til databehandling og kontrol kan hurtigt udvikle sig til overvågning og dermed indgreb i retten til privatliv og beskyttelse af personoplysninger. Der er derfor behov for øget fokus på, hvornår overvågning kan anses for et rimeligt myndighedsmæssigt tiltag i forhold til de legitime, kontrolmæssige formål.

Justitia anbefaler, at Digitaliseringsministeriet/Justitsministeriet i samarbejde med Dataetisk Råd udarbejder et overvågningsetisk reflektionsværktøj, som skal være obligatorisk at anvende for myndighederne, når der skal tages beslutning om tiltag eller ibrugtagelse af ny teknologi, der har

---

[290] Se også Justitias rapport (2024) Ansigtsgenkendelsesteknologi: behov for regulering af politiets anvendelse.
[291] Betænkninger af 9. og 16. maj 2018 til L 68 og L 69, Folketinget 2017-18. Se også rapportens afsnit 5.3.1.

potentiale til f.eks. at øge videoovervågningen i det offentlige rum, eller der overvejes nye muligheder for samkøring og genanvendelse af personoplysninger og udvidelse af eksisterende beføjelser til datasamkøring med henblik på kontrol.

Anbefaling 6: Evaluering af overvågningstiltag med fokus på proportionalitet

På flere områder kan der rejses alvorlig tvivl om, hvorvidt omfanget af overvågning står mål med det konkrete udbytte. Det er imidlertid et grundlæggende krav ved indgreb i retten til privatliv og beskyttelse af personoplysninger, at indgrebet er nødvendigt og ikke kan opnås med mindre indgribende midler (proportionalitet).

Justitia anbefaler, at der i forbindelse med iværksættelse og udvidelse af konkrete overvågningstiltag altid skal være fokus på grundig evaluering af, om formålet med overvågningen opnås. Eksisterende overvågningstiltag skal ikke kunne udvides uden forudgående evaluering af den hidtidige anvendelse og udbytte i forhold til overvågningens formål, herunder om formålet kan opnås med mindre indgribende midler. Det anbefales desuden, at der gennemføres en grundig evaluering af den allerede iværksatte tryghedsskabende videoovervågning med henblik på stillingtagen til, om den omfattende overvågning kan begrænses tidsmæssigt og geografisk. Tilsvarende gælder for nummerpladeovervågning af "no-hits".

Anbefaling 7: Øget gennemsigtighed

Ved indførelse af nye overvågningstiltag mangler der ofte fokus på gennemsigtighed over for borgerne.

Justitia anbefaler, at databeskyttelsesloven ændres, så oplysningspligt over for borgerne i forbindelse med databehandling, som indebærer overvågning, herunder samkøring i kontroløjemed, ikke kan undlades ud fra hensyn til, at dette vil kræve en uforholdsmæssig stor indsats. Derudover anbefales det, at Justitsministeriet sikrer ensartede krav til skiltning for videoovervågning samt sikrer borgerne let adgang til at gøre sig bekendt med, hvem der videoovervåger og til hvilket formål.

10 Referencer

Algorithm Watch (2020): Automating Society 2019. https://algorithmwatch.org/en/automating-society/

Analyse & Tal (2023) *En hverdag af data - En kortlægning af digitale tjenesters dataindsamling, og hvad befolkningen ved og mener om den*. Analyserapport udarbejdet i samarbejde med Dataetisk Råd.

https://www.ogtal.dk/assets/files/En-hverdag-af-data_compressed.pdf

Amnesty International (2024): *Coded Injustice - surveillance and discrimination in Denmarks automated welfare state*

https://amnesty.dk/wp-content/uploads/2024/11/Coded-Injustice-Surveillance-and-discrimination-in-Denmarks-automated-welfare-state.pdf

Betænkning nr. 1345/1997. *Behandling af personoplysninger*. Betænkning afgivet af udvalget om registerlovgivningen.

Blume, P. (2014): *Overvågning. Kan persondataretten gøre nytte?* Nordisk Tidsskrift for Informationsvidenskab og Kulturformidling, årgang 3, nr. 2/3, 2014.

Blume, Peter & Rotmar-Herrmann, Janne (2018): *Ret, privatliv og teknologi*. 4. udgave. Jurist og Økonomforbundets forlag

Brottsförebyggande rådet (BRÅ) (2018): *CCTV and Crime Prevention*. Systematisk Review and Meta-analyse af 80 studier. Udgivet i samarbejde med University of Cambridge

CCTV and Crime Prevention - Brottsförebyggande rådet

CAHAI, Feasibility Study (2020). Udgivet 17. december 2020.

CEPOS (2012) analyse v/ Jacob Mchangama: *Er SKATs beføjelser retsstridige?*

CNBC (2024): Three in four Europeans support use of AI by the police and military.

Datatilsynet (2023): *Brug af kunstig intelligens i den offentlige sektor – kortlægning*.

Det Kriminalpræventive Råd, *Fakta om tv-overvågning*

Effekten af tv-overvågning til opklaring og forebyggelse af kriminalitet - Det Kriminalpræventive råd

European Data Protection Board (EDPB). Retningslinjer 3/2019 om brug af videoudstyr til behandling af personoplysninger. Vedtaget 29. januar 2020

European Data Protection Board (EDPB). Anbefalinger 02/2020 om de europæiske væsentlige garantier for overvågningsforanstaltninger. Vedtaget den 10. november 2020

European Data Protection Board (EDPB). Retningslinjer 5/2022 for anvendelse af ansigtsgenkendelsesteknologi på retshåndhævelsesområdet. Vedtaget den 26. april 2023.

European Union Agency for Fundamental Rights (2019) *Facial recognition technology: Fundamental rights considerations in the context of law enforcement*. Udgivet april 2019.

Eiriksson, B.A. (2008): *Med digitaliseringen øges myndighedernes overvågning af danskerne væsentligt, Hvem tager sig af retssikkerheden*? Ræson, Informations Forlag, 1. juli 2008

Eiriksson, B. A. (2018): *Social digital kontrol er på kant med borgernes ret til privatliv*. Kapitel i Jørgensen, R.F. & Olsen, B.K. (red.): *Eksponeret. Grænser for privatliv i en digital tid*. Gads Forlag.

Justitia (2015): *Udbetaling Danmark: En trussel mod privatlivets fred og retten til databeskyttelse*

Justitia (2017): *Ny skattekontrollov – Har SKAT stadig adgang til fortrolige teleoplysninger?*

Justitia (2019): *Udbetaling Danmarks systematiske overvågning*

Justitia (2019): *Kommunernes Kontrol med modtagere af sociale ydelser*

Justitia (2022): *Retssikkerhed for Digital Udsatte borgere*

Justitia (2024): *Ansigtsgenkendelse – behov for regulering af politiets anvendelse*

Institut for Menneskerettigheder (2016): Forvaltningens kontrol, status 2015-2016

Justitsministeriet (2022). Notat til Folketinget af 25. maj 2022 om betydningen af EU-Domstolens dom af 5. april 2022 i sagen C-140/20, Commissioner of An Garda Síochána m.fl. for de danske logningsregler samt for de retshåndhævende myndigheders indhentning og anvendelse af loggede oplysninger: https://www.ft.dk/samling/20211/almdel/REU/bilag/259/2582271.pdf

Kjær, M.N. (2019): *TV-overvågning og privatlivet. Hvor går grænsen?* Kandidatspeciale, Aalborg Universitet

Kammersgaard Christensen, Tanja (2022): Automatisk Nummerpladegenkendelse (ANPG). Nordisk Tidsskrift for Kriminalvidenskab – nr. 2/2022

Kammersgaard Christensen, T. (2024): *POL-INTEL - er politiets behandling af personoplysninger i overensstemmelse med EU's retshåndhævelsesdirektiv?* Nordisk Tidsskrift for Kriminalvidenskab nr. /2024

Langsted, Lars Bo & Jakobsen, S.S. (2014): *I en højere sags tjeneste. Afvejningen mellem overvågning og privatliv i en retlig kontekst*. Nordisk Tidsskrift for Informationsvidenskab og Kulturformidling, årgang 3, nr. 2/3, 2014, side 41-61.

Lind, Martin Gräs, Hanne Marie Motzfeldt og Charlotte Bagger Tranberg (2008): *Tv-overvågning anno 2008*. Erhvervsjuridisk Tidsskrift 2008.64.

Lorentzen, Peer m.fl. (2011). *Den Europæiske Menneskerettighedskonvention med kommentarer.* 3. udgave. Jurist- og Økonomforbundets Forlag.

Mortensen, H. m.fl (2009): *De overvågede*. Debatbog om overvågning, risici og løsningsmodeller. Udgivet af Forbrugerrådet & DI.

Motzfeldt, Hanne Marie (2018): *Smarte profileringsteknologier og persondataforordningens generalklausul.* Kapitel i Ret SMART – om smart teknologi og regulering, 1. udgave, DJØFs forlag.

Nielsen, K.K. & Lotterup, Anders (2020): *Databeskyttelsesforordningen og databeskyttelsesloven med kommentarer*. 1. udgave. Jurist- og Økonomforbundets Forlag.

Norwegian Human Rights Institution, The Danish Institute for Human Rights & Swedish Institute for Human Rights (2024): *Exploring human rights awareness, attitudes and perception in Scandinavia*

Penney, Jonathon, Chilling Effects: Online Surveillance and Wikipedia Use (2016). Berkeley Technology Law Journal, Vol. 31, No. 1, p. 117, 2016, Available at SSRN: https://ssrn.com/abstract=2769645

Radar, 31. oktober 2024: Juridisk direktør vil undgå mytedannelse, men fastholder lukketheden om Skats AI-profilering | Radar : https://radar.dk/artikel/juridisk-direktoer-vil-undgaa-mytedannelse-men-fastholder-lukketheden-om-skats-ai-profilering

Rigsrevisionen (2015): *Beretning om samarbejdet mellem kommunerne og Udbetaling Danmark*

Rigsrevisionen (2021): *Beretning om politiets patruljering og overvågningskameraer. Afgivet til Folketinget med Statsrevisorernes bemærkninger.*

https://www.ft.dk/-/media/sites/statsrevisorerne/dokumenter/2021/beretning-2-2021-om-patruljering-og-overvaagningskameraer.pdf

Udsen, Henrik (2017): *Danske myndigheders registrering af borgernes adfærd på internettet – regelgrundlaget og de tilhørende kontrolmekanismer*. Rapport udarbejdet i samarbejde mellem Justitia og Københavns Universitet, Det Juridiske Fakultet, Center for informations - og innovationsret

Wired (2023) : How Denmark's Welfare State Became a Surveillance Nightmare | WIRED

Wired (2023) : Inside the Suspicion Machine | WIRED

Wired (2023): This Algorithm Could Ruin Your Life | WIRED

10.1 Noter til tidslinje

[1] Lov | nr. 713 | af 25-06-2014 | Lov om ændring af straffeloven, retsplejeloven og forskellige andre love (styrkelse af indsatsen mod terrorisme og anden alvorlig kriminalitet) | Tilgængelig på: https://www.retsinformation.dk/eli/lta/2014/713.
[2] Information. Politidirektør: Overvågning af biler fanger mest små lovovertrædelser. Sidst opdateret 26. november 2014. https://www.information.dk/indland/2014/11/politidirektoer-overvaagning-biler-fanger-mest-smaa-lovovertraedelser.
[3] Lovforslag | nr. L 41 | af 30-10-2014 | Forslag til lov om ændring af straffeloven, retsplejeloven og forskellige andre love (styrkelse af indsatsen mod terrorisme og anden alvorlig kriminalitet) | Tilgængelig på: https://www.ft.dk/samling/20141/lovforslag/L41/som_fremsat.htm.
[4] EUD af 8. april 2014: Digital Rights-dommen (Forenede sager C-239/12 og C-594/12)
Folketinget. "EU-Domstolen underkender logningsdirektivet." Folketinget, 2014. https://www.ft.dk/samling/20131/almdel/euu/eu-note/22/1357861/index.htm.
[5] Lovforslag | "nr. L 95" | "af" 2014 | Forslag til lov om ændring af udlændingeloven | Tilgængelig på: https://www.ft.dk/samling/20141/lovforslag/l95/20141_l95_som_fremsat.htm.
[6] Bekendtgørelse | nr. 523 | af 29-04-2015 | Lov om ændring af retsplejeloven, straffeloven og forskellige andre love (initiativer rettet mod terrorbekæmpelse mv.) | Tilgængelig på: https://www.retsinformation.dk/eli/lta/2015/523.
[7] Rigsrevisionens beretning om samarbejdet mellem kommunerne og Udbetaling Danmark om kontrolindsatsen (2015)
[8] Justitia (2015): Udbetaling Danmark: En trussel mod privatlivets fred og retten til databeskyttelse
[9] Danske Regering. Et stærkt værn mod terror: Status og initiativer i kampen mod terrorisme. København: Regeringen, februar 2015. https://www.regeringen.dk/media/1312/et_staerkt_vaern_mod_terror.pdf.
[10] Skatteministeriets pressemeddelelse af 28. maj 2015: https://skm.dk/aktuelt/presse-nyheder/pressemeddelelsesarkiv/20150824-slut-med-teleoplysninger. Se også CEPOS analyse fra 2012 v/J. Mchangama: *Er SKATs beføjelser retsstridige?*
Tilgængelig her: https://justitia-int.org/wp-content/uploads/2012/02/2012-02-22-Er-SKATs-bef%C3%B8jelser-retsstridige.pdf
[11] TV 2 Nyheder. Regeringen nedlægger uvildigt terrorlov-udvalg. Sidst opdateret 31. oktober 2015. https://nyheder.tv2.dk/politik/2015-10-31-regeringen-nedlaegger-uvildigt-terrorlov-udvalg.

[12] Lovforslag | "nr. L 83" | "af" 2014 | Forslag til lov om ændring af lov om arbejdsmiljø | Tilgængelig på: https://www.ft.dk/ripdf/samling/20141/lovforslag/l83/20141_l83_efter_2behandling.pdf.
[13] Bekendtgørelse | "nr. 1776" | "af" 16-12-2015 | Bekendtgørelse om politiets anvendelse af automatisk nummerpladegenkendelse (ANPG) | Tilgængelig på: https://www.retsinformation.dk/eli/lta/2015/1776
[14] DR. Overblik: Forstå forslaget om sessionslogning. Sidst opdateret 12. april 2016. https://www.dr.dk/nyheder/politik/overblik-forstaa-forslaget-om-sessionslogning.
[15] Berlingske. Video stopper tyven - men vold forhindrer overvågning ikke. 8. december 2016. https://www.berlingske.dk/samfund/video-stopper-tyven-men-vold-forhindrer-overvaagning-ikke
[16] Institut for Menneskerettigheder: Forvaltningens kontrol, status 2015-2016
[17] EUD af 21. december 2016: Tele2-dommen (Forenede sager C-203/15 og C-C-698/15)
[18] Se bl.a. lovforslag nr. 191 fremsat 26/4 2017 og lovforslag nr. 218 fremsat 11/4 2018.
[19] Lovforslag | nr. L 68 | af 25-10-2017 | 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) | Tilgængelig på: https://www.retsinformation.dk/Forms/R0710.aspx?id=194142.
[20] Lovforslag | nr. L 149 | af 18-05-2017 | Lov om Erhvervsstyrelsens behandling af data | Tilgængelig på: https://www.ft.dk/samling/20171/lovforslag/l149/20171_l149_som_fremsat.htm.
[21] Lovændring | nr. 506 | af 23-05-2017 | Lov om ændring af udlændingeloven | https://www.retsinformation.dk/eli/lta/2017/506
[22] Lovændring | nr. 462 | af 15-05-2017 | Lov om ændring af lov om Forsvarets Efterretningstjeneste (FE) og toldloven | Tilgængelig på: https://www.retsinformation.dk/eli/lta/2017/462.
[23] Lovændring | nr. 671 | af 08-06-2017 | Lov om ændring af lov om politiets virksomhed og toldloven | Tilgængelig på: https://www.retsinformation.dk/eli/lta/2017/671.
[24] Bekendtgørelse | nr. 1078 | af 08-06-2017 | Bekendtgørelse om politiets behandling af oplysninger i forbindelse med tværgående informationsanalyser | Tilgængelig på: https://www.retsinformation.dk/eli/lta/2017/1078.
[25] EU. "Direktiv 98/41/EF om registrering af de ombordværende på passagerskibe, som sejler til og fra havne i Fællesskabets medlemsstater." EUR-Lex, 2017. https://eur-lex.europa.eu/legal-content/DA/TXT/?uri=CELEX:32017L2109.
[26] DR. Kig op: Droner bliver en endnu større del af politiets arbejde i fremtiden. 29. januar 2018. https://www.dr.dk/nyheder/regionale/fyn/kig-op-droner-bliver-en-endnu-stoerre-del-af-politiets-arbejde-i-fremtiden
[27] Lovforslag L13 / 2017. Se L 2017-12-19 nr. 1535 som trådte i kraft 1. januar 2019
[28] Justitias rapport af 20. marts 2017 om skats adgang til fortrolige teleoplysninger Tilgængelig på: https://justitia-int.org/wp-content/uploads/2017/02/Analyse_Ny-skattekontrollov-har-SKAT-stadig-adgang-til-fortrolige-teleoplysninger_20-03-17.pdf
[29] Europa-Parlamentets og Rådets forordning 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandlinger af personoplysninger mv. (GDPR)
[30] Betænkning | BTL 68 og L 69 | af 2017 | Betænkning over: I. Forslag til 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), II. Forslag til lov om ændring af lov om retshåndhævende myndigheders behandling af personoplysninger, lov om massemediers informationsdatabaser og forskellige andre love | Tilgængelig på: https://www.retsinformation.dk/eli/ft/201714L00965.
[31] Lov | nr. 438 | af 08-05-2018 | Lov om Erhvervsstyrelsens behandling af data | Tilgængelig på: https://www.retsinformation.dk/eli/lta/2018/438.
[32] Lovændring | nr. 1706 | af 06-12-2018 | Lov om indsamling, anvendelse og opbevaring af oplysninger om flypassagerer (PNR-loven) | Tilgængelig på: https://www.retsinformation.dk/eli/lta/2018/1706.
[33] Eiriksson, Birgitte Arent. Justitia: Med digitaliseringen øges myndighedernes overvågning af danskerne væsentligt – hvem tager sig af retssikkerheden? RÆSON, 14. november 2018. https://www.raeson.dk/2018/birgitte-arent-eiriksson-justitia-med-digitaliseringen-oeges-myndighedernes-overvaagning-af-danskerne-vaesentligt-hvem-tager-sig-af-retssikkerheden/.
[34] Lovforslag | nr. L 98 | af 2018 | Forslag til lov om ændring af lov om midlertidig regulering af boligforholdene | Tilgængelig på: https://www.ft.dk/samling/20181/lovforslag/l98/index.htm.
[35] Version2. Regeringen dropper masseovervågning af danskernes elforbrug. 28. august 2018. https://www.version2.dk/artikel/regeringen-dropper-masseovervaagning-af-danskernes-elforbrug

[36] Lovforslag | "nr. L 209" | "af" 2018 | Forslag til lov om en aktiv beskæftigelsesindsats | Tilgængelig på: https://www.ft.dk/samling/20181/lovforslag/L209/som_vedtaget.htm.
[37] Lovændring | "nr. 506" | "af" 27-12-2018 | Lov om ændring af lov om tv-overvågning og lov om retshåndhævende myndigheders behandling af personoplysninger | Tilgængelig på: https://www.retsinformation.dk/eli/lta/2018/506.
[38] DR. Politiet holder øje: Videoovervågning skaber flere steder ro i nattelivet. 9. juli 2019. https://www.dr.dk/nyheder/regionale/sjaelland/politiet-holder-oeje-videoovervaagning-skaber-flere-steder-ro-i
[39] Justitia. Høringssvar: Trygheds- og sikkerhedspakken. Justitia, januar 2020. https://justitia-int.org/wp-content/uploads/2020/01/H%C3%B8ringssvar-Trygheds-og-sikkerhedspakken.pdf.
[40] Berlingske. "Københavns Politi: Vi vil gerne bruge ansigtsgenkendelse på borgerne." Berlingske, 23. oktober 2019. https://www.berlingske.dk/indland/koebenhavns-politi-vi-vil-gerne-bruge-ansigtsgenkendelse-paa-borgerne.
[41] Justitia. Analyse: Udbetaling Danmarks systematiske overvågning. Justitia, 8. januar 2020. https://justitia-int.org/analyse-udbetaling-danmarks-systematiske-overvaagning/.
[42] Justitia. Analyse: Kommunernes kontrol med modtagere af sociale ydelser. Justitia, 27. januar 2019. https://justitia-int.org/analyse-kommunernes-kontrol-med-modtagere-af-sociale-ydelser/.
[43] Justitia. Høringssvar: Forbud til dømte seksualforbrydere. Justitia, 13. februar 2019. https://justitia-int.org/hoeringssvar-forbud-til-doemte-seksualforbrydere/.
[44] DR. Undersøgelse i teledataskandale udvides: Nu skal ni års afsluttede straffesager genoptages. DR Nyheder, 8. november 2019. https://www.dr.dk/nyheder/indland/undersoegelse-i-teledataskandale-udvides-nu-skal-ni-aars-afsluttede-straffesager.
[45] L 209 om aktiv beskæftigelsesindsats, som vedtaget 30. april 2019
[46] Skatteudvalgets betænkning af 30. november 2017 til lovforslag nr. L13 om forslag til skattekontrollov. Se L 2017-12-19 nr. 1535 som trådte i kraft 1.januar 2019
[47] EUD af 6. oktober 2020: La Quadrature du Net-dommen (Forenede sager C-511/18, C-512/18 og C-520/18)
[48] Institut for Menneskerettigheder. Kontaktsporingsapps og menneskeretten. Institut for Menneskerettigheder, maj 2020. https://menneskeret.dk/files/media/document/kontaktsporing.pdf.
[49] Justitsministeriet. Aftale om politiets og anklagemyndighedens økonomi 2021-2023. Justitsministeriet, 2020. https://www.justitsministeriet.dk/wp-content/uploads/2020/12/Aftale-om-politiets-og-anklagemyndighedens-oekonomi-2021-2023-1.pdf.
[50] Digitaliseringsstyrelsen. Signaturprojekter med kunstig intelligens i kommuner og regioner. Digitaliseringsstyrelsen. Tilgået 16. december 2024. https://digst.dk/kunstig-intelligens/signaturprojekter/#accordion-malrettede-beskaeftigelsesindsatser-til-ledige-borgere.
[51] Lov nr. 802 af 9. juni 2020, samt ændringslovforslag nr. 102 af 19. maj 2020
[52] Bekendtgørelse | "nr. 2274" | "af" 29-12-2020 | Bekendtgørelse om politiets anvendelse af droner | Tilgængelig på: https://www.retsinformation.dk/eli/lta/2020/2274.
[53] Justitia. Ulovlig logning – Tid til en lovrevision. Justitia, 25. februar 2021. https://justitia-int.org/ulovlig-logning/.
[54] Lovforslag | "nr. L 73" | "af" 2021 | Forslag til lov om ændring af lov om et indkomstregister, skatteindberetningsloven og skattekontrolloven | Tilgængelig på: https://www.ft.dk/samling/20211/lovforslag/l73/index.htm.
[55] Rigsrevisionens beretning af 21. oktober 2021 om politiets patruljering og overvågningskameraer. Tilgængelig her: https://www.rigsrevisionen.dk/Media/637698949985101606/SR0221.pdf
[56] Lovændring | "nr. 873" | "af" 21-06-2022 | Lov om Det Centrale DNA-profilregister og Det Centrale Fingeraftryksregister | Tilgængelig på: https://www.retsinformation.dk/eli/lta/2022/873.
[57] Justitsministeriet. "Ny teknologi skal hjælpe politiet i indsatsen mod seksuelt misbrug af børn." Justitsministeriet, 21 juni 2024. december 2021. https://www.justitsministeriet.dk/pressemeddelelse/ny-teknologi-skal-hjaelpe-politiet-i-indsatsen-mod-seksuelt-misbrug-af-boern/.
[58] Bekendtgørelse | nr. 381 | af 29-03-2022 | Bekendtgørelse om generel og udifferentieret registrering til og med den 29. marts 2023 og opbevaring til og med den 29. marts 2024 af trafikdata | Tilgængelig på: https://www.retsinformation.dk/eli/lta/2022/381.
[59] Justitia. "Thoughts on the DSA: Challenges, Ideas, and the Way Forward through International Human Rights Law." Justitia, 2022. https://justitia-int.org/report-thoughts-on-the-dsa-challenges-ideas-and-the-way-forward-through-international-human-rights-law/.

[60] Institut for Menneskerettigheder. Beretning 2021 - Institut for Menneskerettigheder, juni 2022. Institut for Menneskerettigheder, 2022. https://menneskeret.dk/files/media/document/Beretning%202021%20-%20Institut%20for%20Menneskerettigheder%2C%20juni%202022.pdf.
[61] EUD af 5. maj 2022: Dom om irske logningsregler (C140/20). Se også justitsministerens orientering til Folketinget: https://www.ft.dk/samling/20211/almdel/REU/bilag/259/2582271.pdf
[62] Bkg. nr. 381 af 29/03/2022
[63] Bkg. nr. 380 af 29/3/2022
[64] Højesterets kendelse af 4. oktober 2023 (sag 59/2022)
[65] Justitsministeriet. "Regeringen: Politiet skal kunne bruge genetisk slægtsforskning i efterforskningen." Justitsministeriet, 23. februar 2023. https://www.justitsministeriet.dk/pressemeddelelse/regeringen-politiet-skal-kunne-bruge-genetisk-slaegtsforskning-i-efterforskningen/.
[66] IDA. "Organisationer: EU-forslag om chatkontrol er totalovervågning." IDA, 9. oktober 2023. https://ida.dk/om-ida/nyt-fra-ida/organisationer-eu-forslag-om-chatkontrol-er-totalovervaagning.
[67] Bkg nr. 337 af 28/3/2023
[68] Lovforslag nr. 150, som vedtaget 4. juni 2024 (Gennemførelse af bandepakke IV)
[69] Institut for Menneskerettigheder. "Høringssvar: Ændring af reglerne om logning." Institut for Menneskerettigheder, 24. januar 2024. https://menneskeret.dk/hoeringssvar/aendring-reglerne-logning.
[70] Rigspolitiet. "Politiet styrker brugen af kropskameraer i udvalgte operative opgaver." Rigspolitiet, 22. marts 2024. https://politi.dk/rigspolitiet/nyhedsliste/politiet-styrker-brugen-af-kropskameraer-i-udvalgte-operative-opgaver/2024/03/22.
[71] Europa Kommissionen. AI-forordningen træder i kraft. 1. august 2024. https://commission.europa.eu/news/ai-act-enters-force-2024-08-01_da?utm_source=chatgpt.com
[72] Justitia: Ansigtsgenkendelsesteknologi: Behov for regulering af politiets anvendelse (marts 2024)
[73] Justitsministeriet. Orientering af Folketingets Retsudvalg om politiets brug af ansigtsgenkendelsesteknologi i efterforskning. Justitsministeriet, september 2024. https://www.justitsministeriet.dk/wp-content/uploads/2024/09/Orientering-af-Folketingets-Retsudvalg-om-politiets-brug-af-ansigtsgenkendelsesteknologi-i-efterforskning.pdf.
[74] Akademikerbladet. "Skattestyrelsen mørklægger AI-overvågning af danskerne." Dansk Magisterforening, 22. marts 2024. https://dm.dk/akademikerbladet/aktuelt/ai/2024/skattestyrelsen-moerklaegger-ai-overvaagning-af-danskerne/.
[75] Justitia. "Høringssvar: Omvendt fodlænke." Justitia, 16. december 2024. https://justitia-int.org/hoeringssvar-omvendt-fodlaenke/.
[76] Bkg. nr. 316 af 27/3/2024
[77] L 100 Forslag til lov om ændring af straffeloven og lov om politiets virksomhed. https://www.ft.dk/samling/20241/lovforslag/L100/som_vedtaget.htm

JUSTITIA

DANMARKS UAFHÆNGIGE
JURIDISKE TÆNKETANK