INSTITUT FOR
MENNESKE
RETTIGHEDER

DATA-BESKYTTELSE

STATUS 2015-16

DATABESKYTTELSE
STATUS 2015-16

Denne delrapport er en del af Institut for Menneskerettigheders rapport 'Menneskerettigheder i Danmark, Status 2015-16'. Rapporten behandler udvalgte menneskeretlige emner og giver anbefalinger til forbedring af menneskeretsbeskyttelsen i Danmark.

Rapporten behandler emner om introduktion til menneskeretten, gennemførelse af menneskeretten, asyl, børn, databeskyttelse, etnisk oprindelse, familieliv, forvaltningens kontrol, frihedsberøvelse, handicap, køn, magtanvendelse, religion, retfærdig rettergang, retten til bolig, statsborgerskab, uddannelse, udvisning og udlevering, uregistrerede migranter, væbnet konflikt, ytringsfrihed og ældre.

Rapporten kan læses i sin fulde længde på instituttets hjemmeside, www.menneskeret.dk. Der findes også et sammendrag af rapporten, i trykt form og på hjemmesiden. Rapporten vil løbende blive udbygget, og instituttet modtager gerne kommentarer på statusrapport@menneskeret.dk.

ISBN: 978-87-93241-58-9
EAN: 9788793241589
ISSN: 2445-8996

Danmarks Nationale Menneskerettighedsinstitution

Wilders Plads 8K
1403 København K
Telefon 3269 8888
www.menneskeret.dk

Vi tilstræber, at vores udgivelser bliver så tilgængelige som muligt. Vi bruger fx store typer, korte linjer, få orddelinger, løs bagkant og stærke kontraster.
Vi arbejder på at få flere tilgængelige pdf'er. Læs mere om tilgængelighed på www.menneskeret.dk/tilgaengelighed

INDHOLD

FORKORTELSER

EDPS	Den Europæiske Tilsynsførende for Databeskyttelse
EMD	Den Europæiske Menneskerettighedsdomstol
EMRK	Den Europæiske Menneskerettighedskonvention
ENISA	European Network and Information Security Agency
EU	Den Europæiske Union
EU-chartret	Den Europæiske Unions Charter om Grundlæggende Rettigheder
FE	Forsvarets Efterretningstjeneste
FN	De Forenede Nationer
FTC	USA's føderale handelskommission
ICCPR	FN's konvention om borgerlige og politiske rettigheder
OHCHR	FN's Højkommisær for Menneskerettigheder
PET	Politiets Efterretningstjeneste
PIA	Privatlivsimplikationsanalyse
TEUF	Traktaten om den Europæiske Unions Funktionsmåde
TI	Teleindustrien

KAPITEL 1

1 OVERBLIK

1.1 INDHOLD OG AFGRÆNSNING

Databeskyttelse vedrører beskyttelse af det enkelte menneskes privatliv i forhold til behandling af information. Databeskyttelse skal sikre, at oplysninger, der vedrører borgeren (personoplysninger), kan anvendes på forsvarlig vis i såvel den offentlige som den private sektor. Behovet for beskyttelse af personoplysninger varierer, alt efter hvilken profil og position den enkelte har.

Generelt er det danske samfund kendetegnet ved en høj grad af digitalisering, herunder en omfattende brug af internettet af såvel den enkelte borger som den offentlige forvaltning. Samtidig er den offentlige forvaltning kendetegnet ved en omfattende brug af informationsteknologi (it) kombineret med en entydig identifikation af borgere i form af et cpr-nummer. Dette oplever de fleste som uproblematisk og som et led i en moderne og effektiv offentlig sektor. Der er således en høj grad af tillid mellem borger og stat i Danmark. Set i et databeskyttelsesperspektiv stiller et gennemregistreret og digitaliseret samfund imidlertid skærpede krav til, at de løsninger, standarder og procedurer, der skal beskytte borgerens rettigheder og privatliv, rent faktisk overholdes af såvel offentlige myndigheder som private virksomheder. Når mængden af data, der opsamles og udveksles, stiger, øges tilsvarende sårbarheden over for brud på sikkerhed og databeskyttelse.

Siden 2001 er der i Danmark vedtaget en lang række love og anden regulering med henblik på bekæmpelse af terrorisme og anden alvorlig kriminalitet, der er baseret på en øget udveksling af oplysninger mellem offentlige myndigheder både nationalt og internationalt. De mange nye tiltag i forhold til registrering og udveksling af personoplysninger sætter beskyttelsen af privatliv under pres. Området er komplekst, fordi lovgivningen omfatter mange forskellige sektorer, ligesom udveksling finder sted på såvel nationalt som internationalt plan, ofte uden megen offentlig debat. De seneste års debat om udenlandske og danske efterretningstjenesters adgang til at overvåge danske borgere, eksempler på læk af personoplysninger fra offentlige og private myndigheder, oprustning på cybersikkerhed, EU's domme vedrørende telelogning og safe harbor-ordningen, big data mv. er alle eksempler på, hvorledes databeskyttelse og privatliv i

stigende grad er emner, der rækker ind i alle dele af samfundslivet, og som involverer spørgsmål og afvejninger af både juridisk, teknisk og organisatorisk karakter.

Datatilsynets mandat er begrænset til at føre tilsyn med overholdelse af persondataloven. Der er imidlertid aktuelt ikke noget offentligt organ, som dækker hele den meget brede vifte af problemstillinger, der knytter sig til privatliv og databeskyttelse for såvel offentlige som private virksomheder, når disse problemstillinger falder uden for persondatalovens anvendelsesområde, eller hvor databehandlingen foretages af enheder, der ikke er underlagt Datatilsynets tilsyn. Eksempelvis har Datatilsynet ikke kompetence til at føre tilsyn med efterretningstjenesterne. Ligeledes er der ikke nogen fast praksis for, at lovforslag og offentlige it-systemer forud for deres indførelse skal gennemgå en privacy-vurdering, det vil sige en analyse af mulige implikationer for retten til privatliv. Andre lande, som for eksempel Canada, stiller eksplicitte krav om dette og har en længere tradition på området.[1] Danmarks omfattende digitaliseringsstrategi og den centrale nøgleløsning (NemID) er i modsætning hertil aldrig blevet undergivet en privacy-vurdering.

I denne delrapport behandles nogle af de udfordringer, som Danmark står over for i forhold til borgeres ret til beskyttelse af deres data og kommunikation. Der er fokus på fem temaer, som blandt andet er karakteriseret ved, at de for tiden er under debat/revision. De udvalgte temaer er 1. tele- og internetudbydernes logning af kommunikationsdata, 2. borgeres beskyttelse ved brug af sociale medier, 3. databeskyttelse i den offentlige forvaltning, 4. lagring af personoplysninger via åbne net (cloud computing) samt 5. efterretningstjenesterne og cybersikkerhed.

Andre væsentlige temaer, der ikke behandles her, omfatter blandt andet brug af biometriske data, central lagring af borgeres private nøgler (NemID), udveksling af personoplysninger og datafangst i sundhedssystemet samt udveksling af oplysninger inden for EU og med USA.

Der henvises i øvrigt til delrapporten om forvaltningens kontrol, som indeholder et tema om kontrol med offentlige ydelser. Dette tema indeholder også problemstillinger vedrørende beskyttelse af personoplysninger.

KAPITEL 2

2 DEN INTERNATIONALE RAMME

2.1 RETTEN TIL PRIVATLIV ER EN MENNESKERET

Databeskyttelse er en del af retten til respekt for privatlivet, der blandt andet dækker personlige oplysninger og kommunikation.

Retten til respekt for privatlivet følger af FN's Verdenserklæring om Menneskerettigheder (1948), der slår fast, at "ingen må være genstand for vilkårlig indblanding i private forhold, familie, hjem eller korrespondance, ej heller for angreb på ære og omdømme. Enhver har ret til lovens beskyttelse mod sådan indblanding eller angreb".[2]

En række af FN's konventioner indeholder lignende bestemmelser, der beskytter privatlivet. Det gælder blandt andet FN's konvention om borgerlige og politiske rettigheder (ICCPR), FN's konvention om barnets rettigheder (Børnekonventionen) og FN's konvention om rettigheder for personer med handicap (Handicapkonventionen).[3] I 2015 udnævnte FN's Menneskerettigheds-råd (HRC) for første gang en særlig rapportør for retten til privatliv.[4]

Endvidere er retten til respekt for privatlivet beskyttet i Den Europæiske Menneskerettighedskonventions (EMRK) artikel 8. Retten til respekt for privatlivet er ikke absolut. Der kan lovligt gøres indgreb i retten, hvis der er lovhjemmel hertil, og indgrebet er begrundet i et anerkendt hensyn samt nødvendigt, herunder proportionalt.

Ved siden af EMRK gælder desuden Europarådets konvention om beskyttelse af det enkelte menneske i forbindelse med elektronisk databehandling af personoplysninger (1981), der sikrer særligt retten til privatlivets fred i forbindelse med elektronisk databehandling af personoplysninger. Det fremgår af konventionen, at personoplysninger, som behandles elektronisk, skal:

- indsamles og behandles rimeligt og lovligt
- lagres til nærmere bestemte og lovlige formål og ikke må anvendes på en måde, som er uforenelig med disse formål

- være relevante og tilstrækkelige og ikke omfatte mere, end hvad der kræves i forhold til at opfylde de formål, de er lagret til
- være nøjagtige og om nødvendigt føres ajour
- opbevares i en form, som ikke muliggør identifikation af de registrerede personer længere end nødvendigt i forhold til det formål, de er lagret til.[5]

Konventionen fastsætter også regler om blandt andet adgang til kendskab om elektroniske registre mv. Det bemærkes, at der siden 2011 har været forhandlinger i Europarådets Databeskyttelses-komité om en modernisering af konventionen. Forhandlingerne forventes afsluttet i første halvår af 2016.[6]

Endelig indeholder også Den Europæiske Unions Charter om Grundlæggende Rettigheder (EU-chartret) bestemmelser, der beskytter privatlivets fred. Personlige oplysninger er beskyttet i en særskilt bestemmelse, hvoraf det blandt andet fremgår, at personoplysninger skal behandles rimeligt, til udtrykkeligt angivne formål og på grundlag af de berørte personers samtykke eller på et andet berettiget grundlag fastsat ved lov. Desuden har enhver ret til adgang til indsamlede oplysninger, der vedrører den pågældende, og til berigtigelse heraf.[7] EU-retsakter vedrørende behandling af personoplysninger og den nationale gennemførelse heraf skal respektere bestemmelserne i EU-chartret. Også artikel 16 i Traktaten om den Europæiske Unions Funktionsmåde (TEUF) omhandler databeskyttelse.

EU har i 1995 vedtaget et databeskyttelsesdirektiv, der er grundlaget for den danske persondatalov.[8] På det strafferetlige område er udgangspunktet EU's rammeafgørelse for databeskyttelse inden for politisamarbejde og retligt samarbejde i straffesager fra 2008,[9] der er implementeret i dansk ret.

EU's databeskyttelsesdirektiv har siden 2010 været under revision, blandt andet for at sikre en opdateret og sammenhængende tilgang til databeskyttelse inden for EU.[10] Europa-Parlamentet og Rådet nåede i december 2015 frem til et kompromis omkring reglernes udformning, og databeskyttelsespakken blev formelt vedtaget i april 2016. Den nye databeskyttelsespakke består af en databeskyttelsesforordning[11], der skal erstatte databeskyttelsesdirektivet, og et direktiv om behandling af personoplysninger på det strafferetlige område.[12] Reglerne træder i kraft i maj 2018.[13]

Databeskyttelsesforordningen vil betyde væsentlige ændringer på området. Borgernes rettigheder vil blive forbedret på visse områder, herunder en sikring af retten til "at blive glemt" og til at blive informeret om, hvorvidt person-oplysninger er blevet kompromitteret. Der vil blive indført en fælles europæisk datamyndighed og en "one-stop-shop"-mekanisme, der i visse

grænseoverskridende sager indebærer, at én tilsynsmyndighed vil være enekompetent til at træffe afgørelse i konkrete sager. Tilsvarende vil den lokale myndighed ikke have komperence i disse sager. Forordningen indebærer også, at virksomheder kan idømmes bøder på op til 4% af deres omsætning.

Som led i implementeringen af forordningen vil den eksisterende "Artikel 29-arbejdsgruppe" (nedsat i henhold til EU's databeskyttelsesdirektiv) blive erstattet af den nye europæiske datamyndighed. Artikel 29 gruppen, som aktuelt består af EU-landenes respektive datatilsyn samt Den Europæiske Tilsynsførende for Databeskyttelse, har vedtaget en lang række henstillinger og udtalelser, som forholder sig til aktuelle spørgsmål og lovgivning på databeskyttelsesområdet. Danmark tager del i dette arbejde.

Se endvidere delrapporten om introduktion til menneskeretten.

KAPITEL 3

3 DEN NATIONALE RAMME

3.1 PERSONDATALOVEN SÆTTER REGLERNE

Grundloven indeholder to bestemmelser relateret til privatliv og beskyttelse af personoplysninger. Den ene bestemmelse fastslår, at den enkeltes frihed er ukrænkelig, og den anden bestemmelse understreger boligens ukrænkelighed.[14] Sidstnævnte indebærer, at "husundersøgelse, beslaglæggelse og undersøgelse af breve og andre papirer samt brud på post-, telegraf- og telefonhemmeligheden må, hvor ingen lov hjemler en særegen undtagelse, alene ske efter en retskendelse".[15]

Persondataloven regulerer offentlige og privates behandling af person-oplysninger og skal sikre, at Danmark lever op til EU-reglerne på området. Ved personoplysninger forstås enhver oplysning, der direkte eller indirekte kan henføres til en identificeret eller identificerbar person. Ved behandling forstås enhver aktivitet i tilknytning til en personoplysning. Når den nye databeskyttelsesforordning træder i kraft i 2018, vil persondataloven som udgangspunkt blive erstattet af denne. Der kan dog fortsat være områder, hvor Danmark vælger at lave særskilt regulering, for eksempel på områder hvor den gældende persondatalov indeholder regler, der ikke hidrører fra Persondata direktivet.

Persondataloven indeholder en række regler, som giver den enkelte borger (den registrerede) forskellige rettigheder over for myndigheder, virksomheder, foreninger mv., som behandler oplysninger om den pågældende (den dataansvarlige). Reglerne har til formål at styrke den enkelte borgers retsstilling, blandt andet ved at skabe åbenhed omkring behandlingen af oplysninger og ved at give registrerede personer adgang til at gøre indsigelse over for nærmere bestemte former for behandling af oplysninger. Der gælder forskellige betingelser og procedurer for behandling af personoplysninger afhængig af oplysningernes følsomhed. Uanset graden af følsomhed er der dog en række krav, der altid skal være opfyldt, blandt andet skal oplysningerne være indsamlet med henblik på et sagligt formål. Persondataloven suppleres af en bekendtgørelse om sikkerhedsforanstaltninger til beskyttelse af personoplysninger (sikkerhedsbekendtgørelsen). Sikkerhedsbekendtgørelsen

gælder for offentlige dataansvarlige, mens der ikke er udarbejdet tilsvarende bestemmelser for private virksomheder.[16]

Datatilsynet fører tilsyn med de dataansvarliges overholdelse af persondata-loven. Dette sker ved, at Datatilsynet træffer konkrete afgørelser på baggrund af klager fra borgere, tager sager op på eget initiativ og gennemfører en række inspektioner hos såvel offentlige myndigheder som private virksomheder, der har fået Datatilsynets tilladelse til at behandle personoplysninger. Datatilsynet har også ret til at foretage uanmeldte inspektioner uden retskendelse.

Udviklingen i antallet af oprettede sager hos Datatilsynet i perioden 2009-2013 er angivet i tabel 3.1.

Tabel 3.1 Udviklingen i antallet af oprettede sager hos Datatilsynet 2010-2014[17]

	2010	**2011**	**2012**	**2013**	**2014**	**% stigning 2014 ift. 2013**
Datatilsynets egen administration etc.	237	189	262	237	293	23,6 %
Lovforberedende arbejde	383	339	444	468	519	10,9 %
Forespørgsler og klager – private	1.296	1.235	1.332	1.313	1.265	-3,7 %
Forespørgsler og klager – offentlige	722	730	730	908	975	7,4 %
Sager på Datatilsynets eget initiativ	129	96	118	145	155	6,9 %
Sikkerhedsspørgsmål	52	51	26	14	3	-78,6 %
Internationale sager	168	176	191	188	182	-3,2 %
Kompetence iht. anden lovgivning	18	24	32	68	99	45,6 %
Sager i alt (ekskl. anmeldelser)	3.005	2.840	3.135	3.341	3.491	4,5 %
Private anmeldelser	2.276	2.165	1.734	2.022	1.696	-16,1 %
Offentlige anmeldelser	384	437	297	755	717	-5,0 %
I alt	**5.665**	**5.442**	**5.166**	**6.118**	**5.904**	-3,5 %

KAPITEL 4

4 DEN MENNESKERETLIGE UDVIKLING

Retten til privatliv og databeskyttelse har fyldt meget i den offentlige debat de senere år, både internationalt og i Danmark, navnlig efter Edward Snowdens afsløringer af efterretningstjenesternes massive dataindsamling og -udveksling.

Dette har på FN-niveau foranlediget de første FN-resolutioner om retten til privatliv i en digital tidsalder,[18] og FN's Højkommissær for Menneskerettigheder iværksatte i 2014 en høring om overvågningsrelateret lovgivning og tilsyn på tværs af FN's medlemsstater, hvilket har resulteret i en række anbefalinger på området.[19] Endelig udnævnte FN's Menneskerettighedsråd i 2015 den første særlige rapportør for retten til privatliv.[20]

Databeskyttelse har også været højt på dagsordenen i EU. I oktober 2015 fandt EU-Domstolen den amerikanske Safe Harbor-ordning ugyldig, blandt andet fordi databeskyttelsesniveauet i USA ikke var tilstrækkeligt.[21] Kommissionen og USA indgik i februar 2016 en ny aftale, "Privacy Shield".[22] I december 2015 blev Rådet og Parlamentet enige om et udkast til den nye databeskyttelsesforordning, der sammen med et direktiv om behandling af personoplysninger på det straffe-retlige område udgør EU's nye databeskyttelsespakke.[23] Forordningen stiller blandt andet krav til, at databeskyttelse indtænkes i it-arkitekturen ("privacy by design") og øger fokus på it-sikkerhed hos både offentlige og private institutioner og virksomheder. Pakken er formelt vedtaget i april 2016.

På følgende områder er der siden Status 2014-15 sket positive tiltag:

- I årevis skete der automatisk videregivelse af data om diagnosticering af visse sygdomme fra praktiserende læger til Dansk AlmenMedicinsk Database (DAMD). Indberetningen var begrænset til diabetes og senere også KOL, hjertesvigt og depression. Den vedrørte derfor alene en "nærmere afgrænset" patientgruppe i overensstemmelse med sundheds-loven. På et tidspunkt begyndte der imidlertid at ske automatisk indberetning af alle diagnoser. Der var dermed ikke længere tale om en nærmere afgrænset patientgruppe, og indberetningen var derfor i strid med sundhedsloven. Spørgsmålet var herefter, om de ulovligt indberettede oplysninger alligevel skulle overføres til Rigsarkivet, hvilket

gav anledning til stor debat. I maj 2015 blev dette endeligt afvist, og databasen blev slettet.[24]

- I juli 2015 udnævnte FN's Mennerettighedsråd Joseph Cannataci som den første særlige rapportør for retten til privatliv.[25]

- I december 2015 blev EU-Parlamentet og Rådet enige om et kompromisforslag til den ny databeskyttelsesforordning, der på flere områder styrker borgernes rettigheder og stiller et øget krav til it-sikkerhed. Forordningen blev formelt vedtaget i april 2016 som led i vedtagelsen af databeskyttelsespakken.

Udviklingen har imidlertid også medført nye menneskeretlige udfordringer:

- I 2015 kom det frem, at PET i flere år, uden hjemmel, har indhentet oplysninger om flypassagerer (Passenger Name Record) via SKAT.[26] Hjemmel hertil blev indført i 2015, men PET skal fortsat indhente oplysningerne via SKAT, der således indsamler oplysninger uden for eget myndighedsområde, og dermed oplysninger, de ikke selv har behov for.[27]

- I 2015 fik FE adgang til at overvåge danske borgere i udlandet, såfremt der er bestemte grunde til at formode, at vedkommende deltager i aktiviteter, der kan indebære eller forøge en terrortrussel mod Danmark.[28] FE har ikke hidtil kunne behandle oplysninger om danske borgere, men det kan de nu – med et lavere mistankekrav end i den øvrige strafferetspleje og uden et tilstrækkeligt tilsyn.[29]

- I forlængelse af EU-domstolens underkendelse af logningsdirektivet[30] satte Justitsministeriet spørgsmålstegn ved, hvorvidt de danske regler om sessionslogning var egnede til at opnå deres formål,[31] og besluttede i juni 2014 at afskaffe reglerne.[32] Regeringen arbejdede i 2015-16 på at genindføre sessionslogning uden forinden at evaluere de gældende regler.[33] I marts 2016 meddelte regeringen imidlertid, at sessionslogning i det omfang, regeringen havde påtænkt, vil være for dyrt at indføre. Politiet og Justitsministeriet arbejder derfor videre på et alternativ.[34]

- Regeringen besluttede i oktober 2015 at nedlægge det udvalg af uvildige eksperter, der skulle have gransket den danske antiterrorlovgivning.[35]

- Folketingets Rets- og Kulturudvalg besluttede i juni 2014 at nedsætte en parlamentarisk arbejdsgruppe, der skulle undersøge mulighederne for en bedre datasikkerhed.[36] Arbejdsgruppen afgav i januar 2015 sin endelige

beretning med en række anbefalinger om blandet andet offentlige myndigheders behandling af personoplysninger og tilsynet med databeskyttelse i offentlige myndigheder og private virksomheder.[37] Der er imidlertid endnu ikke fulgt op på arbejdsgruppens anbefalinger.

- Instituttet har tidligere peget på nogle af menneskeretlige problemer, der er forbundet med placeringen af Center for Cybersikkerhed under Forsvarets Efterretningstjeneste (FE). Med vedtagelsen af lov om net- og informationssikkerhed blev Center for Cybersikkerhed tillagt en række tilsynsbeføjelser over for udbydere af net og tjenester, herunder adgang til at gennemføre tilsynsbesøg uden retskendelse.[38] Dette rejser igen spørgsmålstegn ved, om det er berettiget at undtage centret fra de forvaltningsretlige krav, der stilles til andre tilsynsmyndigheder.[39]

KAPITEL 5

5 HER KAN MENNESKERETTIGHEDERNE STYRKES I DANMARK

5.1 LOGNING

I Danmark sker der efter nærmere regler registrering og opbevaring af borgeres kommunikation via telefon og internet, såkaldt logning af trafik- og lokaliserings-data. Reglerne er indført på baggrund af EU-logningsdirektivet fra 2006.

5.1.1 DEN MENNESKERETLIGE BESKYTTELSE

Logning af borgeres kommunikation rejser blandt andet spørgsmål i forhold til retten til respekt for privatliv, der er beskyttet i blandt andet EMRK artikel 8, Europarådets konvention om databeskyttelse og EU-chartret. Desuden er krav til databehandlingen fastlagt i EU's databeskyttelsesdirektiv, der omhandler såvel offentlige institutioner som private virksomheder.

Registrering af oplysninger om den enkelte borgers kommunikation udgør et betydeligt indgreb i borgerens ret til respekt for privatlivet, og der må derfor stilles høje krav til, at nødvendigheden af indgrebet er sandsynliggjort, herunder at indgrebet står i et rimeligt forhold til formålet hermed.

Såvel den Europæiske Tilsynsførende for Databeskyttelse (EDPS) som EU's Artikel 29-gruppe har sat spørgsmålstegn ved, hvorvidt logningsordninger krænker europæiske borgeres ret til privatliv.

Den Europæiske Tilsynsførende for Databeskyttelse understregede i en udtalelse fra 2011 i forbindelse med EU's revision af logningsdirektivet, at opbevaring af telekommunikationsdata udgør et indgreb i retten til privatliv, som hjemlet i EMRK samt i EU-chartret.[40] Endvidere understregede den tilsynsførende, at tilgængeligheden af trafik- og lokaliseringsdata kan være vigtig for efterforskning af terrorisme og andre alvorlige forbrydelser, men udtrykte samtidig tvivl om nødvendigheden af at opbevare data i dette omfang i lyset af individets ret til privatliv og databeskyttelse.[41] På en konference afholdt af EU-Kommissionen i december 2010 refererede den tilsynsførende til logningspligten som "det mest privacy-invaderende instrument, som EU nogensinde har vedtaget, hvad angår omfanget og antallet af mennesker, som det vedrører".[42] En lang række organisationer har rejst en tilsvarende kritik af logningspligten.[43]

Ligeledes udtalte Artikel 29-gruppen som led i den europæiske proces om EU-logningsdirektivet, at logningspligten udgør et omfattende indgreb i samtlige europæiske borgeres ret til privatliv, og at gruppen er forbeholden over for direktivet. Artikel 29-gruppen pointerede, at logning er en historisk nyskabelse, der risikerer at underminere grundlæggende europæiske værdier: "Beslutningen om at opbevare kommunikationsdata med henblik på at bekæmpe alvorlig kriminalitet er uden fortilfælde og af historiske dimensioner. Den griber ind i det daglige liv for samtlige borgere og kan true de grundlæggende værdier og friheder, som alle europæiske borgere nyder og værdsætter".[44] I 2013 blev emnet behandlet i en rapport fra FN's særlige rapportør om ytringsfrihed og retten til privatliv. Rapporten understreger, at der er et påtrængende behov for at revidere national lovgivning, der regulerer staters adgang til kommunikations-data, og sikre, at denne er overensstemmende med de menneskeretlige standarder.[45]

Senest har EU-domstolen i april 2014 erklæret EU's logningsdirektiv fra 2006 for ugyldigt.[46] Domstolen fastslår, at direktivet er i strid med proportionalitets-princippet i forbindelse med retten til respekt for privatlivet og retten til beskyttelse af personoplysninger, som fastsat i EU-chartrets artikel 7 og 8.

5.1.2 DANSKE FORHOLD

Som led i antiterrorpakke I vedtog Danmark i juni 2002 en logningspligt.[47] Logningspligten pålægger teleudbydere at opbevare oplysninger om borgeres kommunikation via telefon og internet i et år.[48] Oplysningerne opbevares hos teleudbyderne og stilles til rådighed for politiet i konkrete sager på grundlag af en retskendelse. Antiterrorpakke I blev hastet gennem Folketinget på grund af det ændrede trusselsbillede efter 11. september 2001, hvorimod det tog fem år, inden logningspligten blev en realitet. Dette skete først i september 2007, da logningsbekendtgørelsen trådte i kraft.[49] Den lange implementeringstid skyldtes blandt andet, at teleudbyderne var stærkt kritiske over for forslaget, fordi det ville påføre dem økonomiske og administrative byrder uden kompensation, men også fordi de blev pålagt at registrere deres kunders kommunikation til brug for efterforskning.

Institut for Menneskerettigheder, Datatilsynet og flere andre påpegede i den forbindelse, at det ikke syntes sandsynliggjort, at logningspligten var et nødvendigt og proportionalt tiltag i et demokratisk samfund.[50] Der kan således sættes spørgsmålstegn ved, om det er effektivt og proportionalt, at man med logningspligten indfører et omfattende indgreb i privatlivsbeskyttelsen, der potentielt rammer alle borgere. Samtidig fritages en række aktører og tjenester fra bekendtgørelsens krav. Bekendtgørelsens mange undtagelser skaber en

retstilstand, hvor en stor gruppe tilfældige borgere registreres, mens de relativt få mistænkte, som man ønsker at ramme med indgrebet, vil kunne undgå logning ved at benytte teletjenester hos en af de institutioner, der er undtaget fra logningspligten.

Logningsbekendtgørelsen gennemfører EU's logningsdirektiv fra 2006.[51] EU-direktivet har gentagne gange været udsat for kritik, blandt andet fra Artikel 29-gruppen. Ligeledes har den østrigske forfatningsdomstol sat spørgsmålstegn ved direktivets overensstemmelse med EU-chartret.[52] I Slovakiet indbragte en gruppe parlamentsmedlemmer direktivet for den slovakiske forfatningsdomstol, ligesom forfatningsdomstole i Tyskland, Cypern, Ungarn, Tjekkoslovakiet og Rumænien har påpeget direktivets hele eller delvise uforenelighed med national lovgivning og/eller med EMRK artikel 8.[53] I maj 2013 afgjorde EU-Domstolen, at Sverige skulle betale 3 mio. euro for forsinkelser med at implementere direktivet i svensk ret.[54] I april 2014 blev logningsdirektivet erklæret for ugyldigt af EU-Domstolen med henvisning til, at det ikke overholdt EU-chartrets bestemmelser.[55] Efterfølgende har den østrigske, slovenske og rumænske forfatningsdomstol erklæret de nationale logningsregler for ugyldige.

Der verserer i øvrigt to sager for EU-Domstolen om henholdsvis de svenske (C-203/15, Tele 2 Sverige AB) og britiske (C-698/15, Davies m.fl.) logningsreglers forenelighed med EU-chartret. Den danske regering har afgivet indlæg i den svenske sag og vil også afgive indlæg i den britiske sag, da sagernes udfald har betydning for de danske logningsreglers forenelighed med EU-chartret.[56]

I lighed med EU-direktivet indeholder også den danske antiterrorlov en revisions-bestemmelse, der angiver, at logningsbekendtgørelsen efter få år skal evalueres med henblik på at sikre, at den lever op til formålet om terrorbekæmpelse. I marts 2010 foreslog den daværende regering at ophæve revisionsbestemmelsen på baggrund af en evaluering foretaget af Justitsministeriet.[57] Det fremgår af lovforslagets bemærkninger, at der var foretaget en evaluering på baggrund af udtalelser fra Rigsadvokaten, Rigspolitiet og Politiets Efterretningstjeneste. Af udtalelserne fremgik blandt andet, at de oplysninger, der blev indhentet med hjemmel i logningsbekendtgørelsen, primært vedrørte kriminalitet, der ikke var terrorrelateret, samt at der kun i meget begrænset omfang blev indhentet data vedrørende internettrafik. Forslaget om at ophæve revisionsbestemmelsen blev mødt med kritik fra en række organisationer, hvoraf flere foreslog, at der i stedet gennemførtes en bredere og mere uvildig evaluering af logningsreglerne. En sådan evaluering af de danske regler er fortsat ikke gennemført (se nærmere herom nedenfor).

Som led i den danske debat har Teleindustrien (TI) flere gange fremført, at registreringen i perioden har udviklet sig dramatisk. Da logningsbekendtgørelsen trådte i kraft i 2007, forventede myndighederne, at der årligt ville blive registreret cirka 15.000 oplysninger pr. borger. Til sammenligning vurderer TI, at der i 2010 blev foretaget cirka 100.000 registreringer pr. borger svarende til cirka 550 mia. registreringer på årsbasis.[58] Dette tal er i 2012 steget til cirka 144.000 registreringer pr. borger, svarende til cirka 900 mia. registreringer på årsbasis, og cirka 3.500 mia. registreringer i 2013.[59]

Som opfølgning på EU-Domstolens underkendelse af EU's logningsdirektiv i april 2014 har Justitsministeriet udarbejdet et notat om dommens betydning for de danske logningsregler.[60] Justitsministeriet finder, at de danske logningsregler samlet set ikke strider mod EU-chartrets artikel 7 og 8. Der sættes dog spørgsmålstegn ved, hvorvidt reglerne om sessionslogning kan anses for egnede til at opnå deres formål, og i juni 2014 besluttede den tidligere regering at afskaffe sessionslogning i Danmark.[61] Allerede i januar 2015 var der imidlertid debat om, hvorvidt sessionslogning skulle genindføres, blandt andet foranlediget af Charlie Hebdo-terrorangrebet i Paris.[62]

Skiftende regeringer har flere gange bebudet en revision af logningsreglerne, senest under det nuværende regeringsprogram.[63] Dette var også tilfældet for den nye justitsminister, der varslede at fremsætte lovforslag om revision af reglerne i foråret 2016.[64] Allerede inden fremsættelsen gav dette kommende lovforslag imidlertid anledning til stor debat,[65] da regeringen varslede at genindføre sessionslogning i en mere vidtgående udgave end den, der blev afskaffet i 2014. Regeringens tanke var, at internetudbyderne skulle registrere kundernes fulde internettrafik, således at politiet ved retskendelse kunne få adgang til oplysninger om, hvilke hjemmesider, en given person havde besøgt, hvor lang tid vedkommende havde brugt på de enkelte sider, og hvor meget der var up- og downloadet fra siden.

Det er blandt andre Institut for Menneskerettigheders opfattelse, at der ville være en række problemer forbundet med dette forslag. For det første ville det medføre registrering af samtlige danske borgere i et langt mere vidtrækkende omfang end hidtil, selvom EU-Domstolen i 2014 fastslog, at generel registrering af samtlige EU-borgeres kommunikation udgør et for vidtgående indgreb i retten til privatliv, også selvom registreringen sker for at bekæmpe alvorlig kriminalitet. Som anført ovenfor, verserer tilmed to sager for EU-Domstolen om lovligheden af nationale logningsordninger, hvis udfald har betydning for de danske regler. For det andet, har regeringen forsat ikke gennemført en grundig evaluering af de eksisterende logningsregler, herunder reglernes afgrænsning og effektivitet.[66]

I marts 2016 annoncerede justitsministeren imidlertid, at det forslag til sessionslogning, som hidtil har været i spil, ifølge en analyse, som Justitstministeriet har fået foretaget af et eksternt konsulentfirma, vil koste omkring en milliard om året. Dette er i justitsministerens optik for dyrt, og Justitsministeriet og Politiet arbejder derfor på at finde en alternativ model.[67] Indholdet af denne kendes dog ikke på nuværende tidspunkt.

Logningsreglerne blev som anført vedtaget som led i terrorpakke I, og der bliver hele tiden vedtaget nye regler, der tillader forskellige former for overvågning af danske borgere med henblik på terrorbekæmpelse. PET har således fået adgang til at indsamle passageroplysninger (Passenger Name Records, PNR),[68] FE har fået adgang til at overvåge danske borgere i udlandet,[69] der er indført adgang for politiet til at benytte automatisk nummerplade genkendelse (ANPG)[70] og senest har det været logningsreglerne, der blev foreslået udvidet. Institut for Menneskerettigheder finder det derfor beklageligt, at regeringen i oktober 2015 valgte at nedlægge det udvalg, bestående af uvildige eksperter, der skulle foretage en granskning af den samlede danske antiterrorlovgivning. Det er også beklageligt henset til, at det blev anbefalet af både Ungarn og Holland (som gentog sin tidligere anbefaling) under Danmarks UPR eksamination i januar 2016.[71] Når der som beskrevet hele tiden bliver indført nye regler, der giver myndighederne adgang til overvågning mv. som led i terrorbekæmpelse, bør der foretages en evaluering – ikke kun af logningsreglerne – men af den samlede antiterrorlovgivning med henblik på at sikre, at reglerne er effektive og ikke hjemler overvågning og andre indgreb i borgernes menneskerettigheder, udover de indgreb der nødvendige og proportionale. Sådan granskning af den danske antiterrorlovgivning bør foretages snarest muligt, og inden der indføres flere antiterrorlove.

5.1.3 ANBEFALINGER

Institut for Menneskerettigheder anbefaler – med henblik på at undgå en krænkelse af menneskerettighederne – at regeringen:

- tager initiativ til en uafhængig evaluering og analyse af de danske lognings-reglers overensstemmelse med EMRK artikel 8 og EU-chartrets artikel 7 og 8. Evalueringen bør blandt andet inddrage og vurdere alternative og mere afgrænsede modeller.

- tager initiativ til en samlet granskning af den danske antiterrorlovgivning.

5.2 SOCIALE MEDIER

Sociale medier som for eksempel Facebook, der er en amerikansk virksomhed med europæisk kontor i Irland, foretager en omfattende indsamling af oplysninger om Facebookbrugere, herunder europæiske brugere, hvilket rejser særlige udfordringer i forhold til den europæiske databeskyttelse.

5.2.1 DEN MENNESKERETLIGE BESKYTTELSE

I forhold til menneskeretten vedrører brugen af sociale medier retten til respekt for privatliv, der er beskyttet i blandt andet EMRK artikel 8, Europarådets konvention om databeskyttelse og i EU-chartret. Sociale mediers indsamling af oplysninger om europæiske brugere og deres behandling og udveksling af personoplysninger kan potentielt krænke den enkeltes ret til privatliv og data-beskyttelse efter de standarder, der er fastlagt i EU's persondatadirektiv. Private virksomheders behandling af personoplysninger er omfattet af EU's persondata-direktiv på linje med offentlige institutioner.

I juni 2009 afgav Artikel 29-gruppen en udtalelse om, hvorledes den europæiske databeskyttelse påvirker sociale medier som Facebook og Myspace.[72] I udtalelsen understreges det, at sociale medier er ansvarlige under EU's databeskyttelsesdirektiv, herunder at brugere kun må uploade billeder og information om andre personer med udtrykkeligt samtykke fra den pågældende. Endvidere anbefaler Artikel 29-gruppen, at sociale medier indhenter samtykke, før de anvender indsamlet data til markedsføring og lignende. I forhold til personfølsomme oplysninger må disse ikke behandles eller videregives, og brugere skal generelt have mulighed for at skrive under pseudonym. Artikel 29-gruppen fremhæver, at særlig opmærksomhed bør rettes mod beskyttelsen af mindreårige, der benytter sociale medier. Ligeledes understreges det, at sociale medier er underlagt EU's databeskyttelsesdirektiv, uanset om deres kontorer befinder sig uden for Europa.[73]

Efterfølgende har EU-kommissionen støttet op om Artikel 29-gruppens anbefalinger og har som led i revisionen af EU's databeskyttelsesdirektiv foreslået at skærpe håndhævelsen over for private virksomheder.

Også Europarådet har fokus på sociale medier. Europarådet har i april 2012 vedtaget en anbefaling, som angiver en række tiltag, der kan styrke menneske-rettighederne i forbindelse med brug af sociale medier.[74] Anbefalingen understreger blandt andet, at medlemsstaterne skal sikre, at brugerne gøres bekendt med betingelserne for at deltage i sociale medier i en form, som er umiddelbart tilgængelig. Som led heri skal brugerne informeres om de konsekvenser, det måtte have for ytrings- og informationsfriheden samt retten

til privatliv. Det anbefales, at en særlig oplysningsindsats skal rettes mod forældre og lærere.

5.2.2 DANSKE FORHOLD

Brugen af sociale medier som for eksempel Facebook har været markant stigende i Danmark de seneste år, hvilket rejser en række udfordringer i forhold til den enkelte borgers privatliv og databeskyttelse. Et af diskussionspunkterne har været spørgsmålet om jurisdiktion, og hvorledes man kan håndhæve EU's persondatadirektiv over for amerikanske virksomheder. Et andet punkt vedrører Facebooks regulering af ytringsfriheden.

Facebook har cirka 3 mio. brugere i Danmark og 30.000 i Grønland. Facebook fungerer ved, at brugeren opretter en profil og under denne publicerer diverse informationer, musik, billeder mv., som alt efter den enkeltes indstillinger enten er rettet mod brugerens "venner" eller er generelt tilgængelige. Facebook har ved flere lejligheder understreget, at de overholder EUs persondatadirektiv. Reglerne giver imidlertid en vid adgang til at bruge og viderebringe person-oplysninger, når den enkelte har samtykket til det. Dette samtykke gives, når brugeren accepterer tjenestens erklæring om rettigheder og ansvar, herunder deres privatlivspolitik. Facebooks privatlivspolitik understreger, at der opsamles en lang række oplysninger om den enkelte bruger, og at disse kombineres med oplysninger om brugerens venner og andre for at kunne foreslå en række forskellige tjenester. De vilkår, som brugeren samtykker til, er imidlertid svære at gennemskue, og Facebook er gentagne gange blevet kritiseret for deres behandling af personoplysninger (se nedenfor).

Institut for Menneskerettigheder, DR, Berlingske Media, Forbrugerrådet og Medierådet for Børn og Unge gennemførte i 2013 en repræsentativ undersøgelse af 327 unge og 404 forældres brug af sociale medier, deres håndtering af privatlivet, når de bruger disse, og deres holdninger og bekymringer i forhold til privatlivets nye vilkår på de sociale medier. Undersøgelsen viste, at 98 procent af de unge har en profil på de sociale medier, heraf 94 procent på Facebook. 51 procent af de unge tillægger det stor betydning, at de data, de deler, ikke bliver set eller brugt af nogen, de ikke kender. Samtidig føler kun 24 procent sig sikre på, at deres data ikke bliver delt eller brugt af en bredere kreds, end de selv har ønsket.[75] Undersøgelsen blev i november 2013 fulgt op af fokusgruppeinterviews på gymnasier i Aarhus og Københavnsområdet[76] samt i 2014 af en vejledning (FAQ) om ret og ansvar på sociale medier.[77]

De nordiske datatilsyn kontaktede i juli 2011 Facebook for at få større klarhed over virksomhedens behandling af personoplysninger.[78] Af Facebooks svar til det

norske datatilsyn i september 2011 fremgår det blandt andet, at brugernes profiloplysninger som udgangspunkt er offentlig information, som Facebook kan dele med de virksomheder, Facebook samarbejder med, medmindre brugeren aktivt gør sine såkaldte privatlivsindstillinger mere restriktive. Ligeledes understreges det, at de opslag, som brugeren har på sin væg, indgår som led i målrettet markedsføring og kan udnyttes af de virksomheder, som Facebook samarbejder med.[79]

Der er aktuelt stor variation i, hvorledes de europæiske landes datatilsyn håndhæver den nationale persondatabeskyttelse over for sociale medier som Facebook. Eksempelvis har det tyske datatilsyn i flere sager stillet krav til såvel myndigheder som Facebook. Datatilsynet i Hamburg har krævet, at Facebook fjerner deres funktion til ansigtsgenkendelse, og datatilsynet i Slesvig-Holsten har varslet bøder til offentlige myndigheder, der ikke fjerner deres Facebook-sider og tilhørende "synes godt om"-knapper på deres hjemmesider. I februar 2013 afgjorde en administrativ domstol i Slesvig-Holsten, at Facebook skal opfylde den irske persondatalovgivning, idet Facebook har europæisk hovedkontor i Dublin. Domstolen mener ikke, at der kan stilles krav til Facebook efter tysk persondata-lov, idet Facebook ikke behandler personoplysninger i Tyskland. Datatilsynet fra Slesvig-Holsten har udtrykt forundring over afgørelsen, og henvist til at Facebook heller ikke behandler persondata i Irland (dette sker alene i USA).[80]

I oktober 2011 anlagde Max Schrems, en jurastuderende fra Østrig, sag mod Facebook i Irland for at have gemt data, som han havde slettet fra sin profil. Ligeledes klagede en dansker i marts 2011 over, at man kunne indmeldes i en Facebook-gruppe uden at have givet samtykke. Begge klager indgik i en tre-måneders-inspektion, som det irske tilsyn foretog i efteråret 2011 hos Facebook i Irland, og som resulterede i en rapport og en række anbefalinger til Facebook. Facebook har efterfølgende givet tilsagn om at følge flere af anbefalingerne med henblik på at styrke databeskyttelsen, herunder at skærpe praksis vedrørende sletning af data og sikre, at den enkelte ikke kan indmeldes i grupper uden at have givet tilsagn.[81] Senest har Max Schrems i august 2014 organiseret et gruppesøgsmål mod Facebook for krænkelser af EU-borgeres ret til privatliv. Søgsmålet fik i løbet af den første uge 25.000 underskrifter.[82] Den stærkt omtalte sag blev i 2015 afvist en østrigsk distriktsdomstol (under henvisning til manglende jurisdiktion), men Schrems ankede, og appelinstansen afviste argumentet om manglende jurisdiktion og afsagde dom til fordel for Schrems. Herudover har der været rejst spørgsmål om, hvorvidt søgsmålet kan rejses som et gruppesøgsmål i henhold til EU's procedure regler. Dette spørgsmål verserer aktuelt for den østrigske højesteret. Herudover fik Schrems i oktober 2015 EU-domstolens ord på, at den overførsel der sker af europæers personoplysninger til Facebook i USA ikke kan retfærdiggøres med henvisning til Safe Harbor aftalen.

Sagen var oprindelig indbragt for det irske datatilsyn, der afviste sagen, men EU-domstolen fastslog, at det irske datatilsyn skulle have undersøgt sagen. Domstolen erklærede samtidig Safe-Harbor aftalen for ugyldig.[83] Se nærmere herom i afsnit 5.4.

I november 2011 indgik USA's føderale handelskommission (FTC) et forlig med Facebook i USA, hvorefter virksomheden forpligter sig til at skærpe beskyttelsen af brugernes privatliv, herunder undergå en uafhængig revision af deres praksis vedrørende personoplysninger de næste 20 år.[84]

I Danmark stiller Datatilsynet ikke krav til Facebook, men opfordrer i stedet danske brugere til at kontakte Facebook direkte. Det fremgår af Datatilsynets hjemmeside, at "hvis du er utilfreds med noget, som et socialt netværk gør som dataansvarlig, skal du i første omgang kontakte det sociale netværk og forklare, hvad det handler om. Det gælder også, hvis du ønsker at få din profil slettet – det må du tage op med det sociale netværk, og du skal måske give dem flere oplysninger, så de er sikre på, at du er berettiget til at kræve profilen slettet".[85] Dette skyldes ifølge Datatilsynet, at Facebook er hjemhørende i Irland og således uden for dansk jurisdiktion. Denne praksis står i kontrast til den mere offensive praksis i lande som Tyskland og Frankrig og viser, at der aktuelt er stor variation i, hvorledes de nationale datatilsyn forholder sig til internetbaserede tjenester, der retter sig mod et givet land og sprogområde, men har kontor uden for landets grænser.

Den aktuelle praksis, hvorefter danske brugere, der oplever deres rettigheder krænket, er henvist til at rette henvendelse til Facebook og eventuelt klage via det irske datatilsyn, giver i praksis en minimal beskyttelse af den enkelte. Dette på trods af at Facebook retter sig mod det danske marked og indsamler oplysninger fra mere end 3 mio. danske brugere. Som led i den nye persondata-forordning vil Datatilsynet skulle spille en mere aktiv rolle ift. at bistå danske brugere med at få sager behandlet, i samarbede med det irske Datatilsyn.

En anden udfordring vedrører Facebooks forhold til ytringsfriheden.

I udgangspunktet er forholdet mellem et socialt medie som Facebook og dets brugere et privatretligt forhold, hvor det sociale medie kan fastsætte rammerne for aftalen gennem et sæt standardvilkår. Af Facebooks standardvilkår fremgår det blandt andet, at Facebook forbeholder sig ret til at fjerne indlæg, der opleves som stødende eller krænkende, uagtet at disse er lovlige. Dette står i kontrast til det "almindelige" offentlige rum, hvor hensynet til borgernes ytringsfrihed vejer tungt, og hvor indgreb i ytringsfriheden skal have hjemmel i lov. Facebook kan således de facto definere et mere begrænset rum for ytringsfriheden.

Samtidig har Ombudsmanden i 2011 fastslået, at skriverier på Facebook betragtes som en "offentliggørelse", hvis disse er tilgængelige for en bredere kreds.[86] Ombudsmanden har udtalt, at oplysninger på Facebook kan være offentligt tilgængelige på mange måder afhængig af for eksempel ens privatlivs-indstillinger og antallet af ens Facebook-venner. Man må altså foretage en konkret afvejning, blandt andet ud fra hvor lettilgængelige oplysningerne er, og hvor mange der har adgang til dem.

Er der en bred adgang til oplysningerne og dermed tale om offentliggørelse, vil man kunne blive dømt efter straffelovens bestemmelser, for eksempel § 266 b (om hadefulde ytringer) eller § 267 (beskyttelse mod æreskrænkelser). Der foreligger således en situation, hvor brugeren på den ene side begrænses i sin ytringsfrihed via den privatretlige aftale med Facebook og samtidig skal stå til ansvar for sine ytringer på tilsvarende vis som i andre offentlige fora. Forholdet mellem sociale medier og ytringsfriheden blev blandt andet debatteret på en høring om internetcensur i Europahuset i november 2013, med deltagelse af Facebook og Google,[87] samt på en høring om censur på nettet og beskyttelse af private data i Kulturudvalget i marts 2014.[88]

Der henvises i øvrigt til delrapporten om ytrings- og forsamlingsfrihed.

Det kan altså være vanskeligt for den enkelte borger, navnlig børn og unge, at overskue sine rettigheder, når man færdes på de sociale medier. Medierådet for Børn og Unge har i samarbejde med Forbrugerrådet Tænk, Institut for Menneskerettigheder, Digital Identitet, Danish Science Factory og Børnerådet på baggrund af Europarådets guide til internetbrugerne udarbejdet "Din guide til menneskerettigheder på internettet", som er særligt målrettet børn og unge, og som også vedrører sociale medier.[89] Henset til omfanget af brugen af sociale medier, og de menneskeretlige problemstillinger, der er knyttet hertil, er der imidlertid herudover brug for en redegørelse, der mere specifikt forholder sig til brugernes, herunder børn og unges, rettigheder og vilkår på de sociale medier. På samme vis er der behov for en udførlig redegørelse for, hvordan og i hvilket omfang man kan klage til sociale medier, som for eksempl Facebook.

5.2.3 ANBEFALINGER

Institut for Menneskerettigheder anbefaler – med henblik på at fremme menneskerettighederne – at Danmark:

- udarbejder materiale, som på en lettilgængelig måde redegør for brugerens rettigheder og vilkår, herunder klageadgang, ved brug af sociale medier som

Facebook. Materialet bør blandt andet tage sigte mod lærere og elever i folkeskolen.

Institut for Menneskerettigheder anbefaler – med henblik på at fremme menneskerettighederne – at Datatilsynet:

- undersøger, hvordan det danske tilsyn med sociale mediers opbevaring og udveksling af personoplysninger kan skærpes.

5.3 DATABESKYTTELSE I DEN OFFENTLIGE FORVALTNING

Den stigende digitalisering i det danske samfund sætter skærpede krav til en effektiv og tidsvarende beskyttelse af personoplysninger i den offentlige forvaltning. De seneste års mange eksempler på brud på datasikkerhed illustrerer behovet for mere grundlæggende at forbedre sikkerheden ved behandling af personoplysninger i den offentlige sektor.

5.3.1 DEN MENNESKERETLIGE BESKYTTELSE

Offentlige myndigheders behandling af personoplysninger skal iagttage EMRK artikel 8, Europarådets konvention om beskyttelse af det enkelte menneske i forbindelse med elektronisk databehandling af personoplysninger samt EU-chartret og EU's databeskyttelsesdirektiv. Disse instrumenter fastsætter udtrykkelige krav til databeskyttelsesmæssige garantier for den berørte borger.

Retten til privatliv har de seneste år været højt på den internationale menneskeretlige dagsorden, ikke mindst foranlediget af Edward Snowdens afsløringer af efterretningstjenesten, NSA's omfattende overvågning. I december 2013 vedtog FN's generalforsamling den første resolution om retten til privatliv i en digital tidsalder.[90] Resolutionen understreger blandt andet, at den stigende brug af it forøger staternes mulighed for at indsamle personoplysninger og overvåge borgere på måder, der krænker den enkeltes ret til privatliv. Staterne opfordres derfor til at sikre, at lovgivning vedrørende indsamling og brug af personoplysninger respekterer de menneskeretlige standarder for ret til privatliv. Samtidig understreges betydningen af et effektivt og uafhængigt tilsyn på nationalt plan. Som opfølgning på resolutionen har FN's Højkommissær for Menneskerettigheder (OHCHR) indsamlet data om nationale forhold og fremlagde i juni 2014 en rapport, der forholder sig meget kritisk til den praksis, der eksisterer i mange lande. Rapporten fremhæver blandt andet manglende transparens og retssikkerhed knyttet til statslig dataindsamling og potentiel overvågning.[91] Efterfølgende har FN's generalforsamling vedtaget en opfølgende resolution om retten til privatliv i november 2014.[92]

5.3.2 DANSKE FORHOLD

Der har de senere år været flere sager, der involverer læk af personoplysninger, herunder læk af cpr-numre og personoplysninger om elkunder, hacking af kørekortregistret, fejlagtige udleveringer af sundhedsoplysninger, fejlagtig offentliggørelse af personoplysninger fra flere kommuner mv.

Særligt CSC-sagen har fået meget opmærksomhed. Sagen vedrørte hacker-angrebet i 2012 på virksomheden CSC, der varetager driften af en række informationssytemer for blandt andet Rigspolitiet som dataansvarlig for Kriminal-registret, Kørekortsregistret og Pasregistret samt Schengeninformationssytemet. Sidstnævnte inderholder oplysninger om personer, der er eftersøgt, har indrejse-forbud i Schengenområdet eller er under overvågning af politi eller efterretnings-tjenester. Persondata fra disse registre blev lækket, og i relation til Schengen-informationssystemet udtalte Datatilsynet i juli 2015 en hård kritik af Rigspolitiet for ikke at have truffet de fornødne sikkerhedsforanstaltninger til at forhindre et sådant angreb og for dermed ikke at have levet op til persondataloven og Schengenkonventionen.[93]

Rigsrevisionen har også af flere omgange udtalt kritik af it-sikkerheden hos flere offentlige institutioner. Af Rigsrevisionens beretning fra november 2013 fremgik det blandt andet, at flere statslige virksomheder havde et utilstrækkeligt it-sikkerhedsniveau og en mangelfuld beskyttelse af persondata.[94] Beretningen var baseret på 42 it-revisioner i statslige virksomheder i 2012. Rigsrevisionen fremhævede blandt andet Statens IT, Rigspolitiet og Statens Serum Institut, men understregede, at man vurderede, at det mangelfulde it-sikkerhedsniveau og den utilstrækkelige beskyttelse af personoplysninger gjaldt en større gruppe af statslige institutioner. En tilsvarende kritik blev rejst af Rigsrevisonen i november 2014 på baggrund af undersøgelser i otte statslige institutioner, herunder Danmarks Statistik, Rigspolitiet og SKAT.[95] På baggrund af undersøgelser i yderligere seks institutioner, herunder Statens IT, konkluderede Rigsrevisionen igen i oktober 2015, at de seks institutioner ikke havde efterlevet en række anerkendte anbefalinger for god it-sikkerhedspraksis, men at institutionerne havde oplyst, at de siden da havde foretaget en række kompenserende tiltag.[96]

Som opfølgning på blandt andet Se og Hør-sagen, vedrørende læk af oplysninger om kendte mennesker og andres brug af kreditkort, afgav Retsudvalget og Kulturudvalget den 3. juni 2014 en beretning om nedsættelse af en parlamentarisk arbejdsgruppe, der skal undersøge mulighederne for en bedre beskyttelse af personfølsomme oplysninger og et effektivt tilsyn med offentlige institutioner såvel som private virksomheders behandling af disse.[97] Beretningen opfordrer blandt andet regeringen til at indkalde til forhandlinger om at styrke Datatilsynet, at udvide mandatet for det tværministerielle udvalg, der skal

kortlægge sikkerhedsproblemer ved betalingskort, til at omfatte alle områder, hvor der opbevares personfølsomme oplysninger, at prioritere persondata-beskyttelsen højt i den kommende EU-regulering på området (som beskrevet nedenfor) og at udarbejde en årlig redegørelse for datasikkerhed til Folketinget. Arbejdsgruppen skal inddrage eksterne eksperter, herunder Forbrugerombudsmanden, Forbrugerrådet Tænk, Rådet for Digital Sikkerhed samt Institut for Menneskerettigheder. Arbejdsgruppen har afholdt et dialogmøde med de eksterne eksperter i august 2014 samt to offentlige høringer i oktober og november 2014. På høringen i oktober understregede Datatilsynet blandt andet, at tilsynets inspektioner generelt viser en mangelfuld efterlevelse af persondataloven og sikkerhedsbekendtgørelsen[98] hos de offentlige institutioner.[99] Arbejdsgruppen afgav sin endelige beretning i januar 2015 med en række anbefalinger, herunder styrkelse af tilsynsmyndigheder, øgede sanktionsmuligheder ved brud på datasikkerhed, samling af ansvaret for datasikkerhed, og tekniske krav til sikring af følsomme personoplysninger.[100] Institut for Menneskerettigheder må dog desværre konstatere, at der ikke efterfølgende er fulgt op på arbejdsgruppens anbefalinger.

Siden 2011 har regeringen på EU-niveau forhandlet et forslag til en databeskyttelsesforordning, der sigter mod at harmonisere og opdatere reglerne for databeskyttelse i EU til erstatning for det nuværende Persondatadirektiv fra 1995.[101] De nye regler sigter blandt andet mod en øget beskyttelse af borgeren ved brug af internetbaserede tjenester såsom sociale medier. En forordning finder, i modsætning til et direktiv, umiddelbart anvendelse i medlemslandene, uden at den skal implementeres i dansk ret. Dette betyder, at persondataloven skal ophæves, når forordningen bliver sat i kraft. Efter mere end 4.000 ændringsforslag til det oprindelige udkast vedtog EU-Parlamentet i marts 2014 et kompromisforslag.[102] I december 2015 blev Rådet og Europa-Parlamentet enige om et udkast til forordningen, der sammen med et direktiv om behandling af personoplysninger på det strafferetlige område udgør EU's nye databeskyttelses-pakke.[103] De nye regler lægger blandt andet op til, at der i visse situationer stilles krav om obligatorisk privacy-vurdering (privacy impact assessment – PIA) forud for indførelse af it-løsninger i såvel den offentlige forvaltning som i virksomheder (se nedenfor vedr. PIA). Der foreslås ligeledes indført et princip om "Privacy by Design" (privatlivsbeskyttelse indbygget i it-arkitekturen) for at sikre, at der tages hensyn til databeskyttelsen allerede i planlægningsfasen ved nye it-systemer. Forordningen indfører også en pligt for offentlige myndigheder og visse private virksomheder til at udpege en databeskyttelsesansvarlig, der skal sikre, at forordningens krav efterkommes. Pakken er formelt vedtaget i april 2016.

Teknologirådet har tilbage i 2005 anbefalet, at der gennemføres en PIA forud for indførelse af it-løsninger i den offentlige forvaltning.[104] En PIA skal vurdere,

hvilke konsekvenser systemerne har for de praktiske muligheder for at leve op til "god databehandlingsskik" og øvrige persondataregler. Ligeledes har den daværende IT- og Telestyrelse i samarbejde med Dansk Industri (ITEK) lavet en skabelon for gennemførelse af PIA, primært rettet mod it-kunder og leverandører,[105] og Digitaliseringsstyrelsen har udsendt "Guide til konsekvensvurdering af privatlivs-beskyttelse"[106] samt "Vejledning i vurdering af offentlige it-projekters potentielle konsekvenser for privatlivet".[107] Senest har ITEK i oktober 2014 udarbejdet en vejledning til, hvorledes virksomheder og offentlige institutioner kan gennemføre PIA, baseret på internationale standarder.[108] Der er i dag ikke krav til offentlige myndigheder om at udarbejde en privacy-vurdering forud for indførelse af nye it-løsninger, der behandler personoplysninger. Dog følger det af sikkerhedsstandarden ISO 27001, som statslige it-projekter skal følge, at behandlingen af personoplysninger skal inddrages i risikovurderingen. Privacy-vurderinger har i flere år været fast praksis i lande som Canada. Den canadiske model adskiller sig fra Digitaliseringsstyrelsens guide derved, at risikovurderingen tager udgangspunkt i borgerens krav på beskyttelse. Dette indebærer, at borgeren ikke skal identificeres, medmindre det er strengt nødvendigt i den konkrete situation.

5.3.3 ANBEFALINGER

Institut for Menneskerettigheder anbefaler – med henblik på at fremme den enkeltes menneskerettigheder – at Digitaliseringsstyrelsen:

- sikrer en obligatorisk praksis for PIA og "privacy by design", som led i implementeringen af den nye persondataforordning, forud for indførelse af it-løsninger, der behandler personoplysninger i den offentlige sektor.

- i samarbejde med Datatilsynet sikrer et effektivt tilsyn med, at offentlige it-projekter og deres leverandører efterlever de standarder for sikkerhed og databeskyttelse, der er foreskrevet i persondataforordningen, sikkerhedsbekendtgørelsen og ISO 27001.

5.4 CLOUD COMPUTING

Cloud computing er en relativt ny form for dataopbevaring og indebærer en "internetbaseret adgang til en delt pulje af konfigurerbare it-ressourcer (net, servere, datalager, programmer og services)".[109] Dette betyder, at data placeres i en elektronisk tjeneste ("en sky"), typisk sammen med andre data, på en lokalitet, hvor personen ikke har fysisk adgang til data og systemer. Cloud computing rejser nogle principielle problemstillinger i forhold til behandling og beskyttelse af personoplysninger.

5.4.1 DEN MENNESKERETLIGE BESKYTTELSE

Offentlige myndigheders behandling af personoplysninger skal iagttage EMRK artikel 8, Europarådets konvention om beskyttelse af det enkelte menneske i forbindelse med elektronisk databehandling af personoplysninger samt EU-chartret og EU's databeskyttelsesdirektiv, uanset den konkrete it-løsning. Disse instrumenter fastsætter udtrykkelige krav til databeskyttelsesmæssige garantier for den berørte borger.

Cloud computing-tjenester skal, på linje med andre it-løsninger, efterleve de standarder, der er fastlagt i EU's persondatabeskyttelsesdirektiv samt persondataloven, herunder iagttage de skærpede beskyttelseskrav, som stilles i forbindelse med følsomme personoplysninger.

I en udtalelse fra juli 2012 analyserede Artikel 29-gruppen brug af cloud computing i lyset af EU's persondatabeskyttelse. Gruppen konkluderede blandt andet, at virksomheder og offentlige instanser, der ønsker at bruge cloud-tjenester, bør gennemføre en omfattende risikovurdering forud for indførelsen af sådanne tjenester. Den anbefalede endvidere, at der kun benyttes en cloud-tjeneste, som forpligter sig til at overholde EU's persondatalovgivning, og som kan garantere lovligheden af eventuelle internationale dataoverførsler.[110]

I udgangspunktet må der kun overføres oplysninger til et tredjeland, såfremt dette land sikrer et tilstrækkeligt beskyttelsesniveau. Kommissionen kan fastslå, at dette er tilfældet på grundlag af landets lovgivning og internationale forpligtelser. Kommissionen fastslog således i 2000, at USA, inden for rammerne af den amerikanske safe harbor-ordning (en række principper for data-beskyttelse, som amerikanske virksomheder kan tilslutte sig på frivillig basis), sikrede et tilstrækkeligt beskyttelsesniveau.

Som nævnt under afsnit 5.2 underkendte EU-domstolen i 2015 Safe Harbor aftalen mellem EU og USA. Domstolen fandt, at Kommissionens beslutning, om at USA var et sikkert tredjeland, var ugyldig, blandt andet henset til, at den amerikanske safe harbor-ordning var frivillig, kunne tilsidesættes af hensyn til statens sikkerhed mv., og at ordningen ikke i tilstrækkeligt grad sikrede borgernes ret til privatliv og adgang til effektive retsmidler.[111]

På denne baggrund har Kommissionen i starten af februar 2016 indgået en ny aftale med USA, "Privacy Shield". Aftalen blev offentliggjort den 29. februar 2016 og har til hensigt at skabe stærke forpligtelser for virksomheder, en solid håndhævelse, klare beskyttelsesmekanismer, gennemsigtighed i relation til den amerikanske regerings adgang til data, en effektiv beskyttelse af EU-borgerne med klageadgang og en årlig revision. Kommissionen hæfter sig ved, at USA for

første gang har afgivet bindende tilsagn om, at adgangen til persondata som led i efterretningsindsatser vil være klart begrænset og kontrolleret, ligesom de europæiske borgere vil blive beskyttet mod masseovervågning.[112] Aftalen skal vedtages af Rådet efter Europa-Parlamentets godkendelse, men inden da skal Medlemsstaterne og Artikel 29-grupen konsulteres. Max Schrems mener dog ikke, at den nye aftale sikrer EU-borgernes data i tilstrækkeligt omfang.[113]

5.4.2 DANSKE FORHOLD

Cloud computing blev i 2010 behandlet af regeringens it-sikkerhedskomite, der udgav rapporten "Sikkerhed i Cloud Computing".[114] Emnet var ligeledes på Artikel 29-gruppens arbejdsprogram for 2010/2011.

Datatilsynet har flere gange forholdt sig til cloud computing: I 2010 på baggrund af en henvendelse fra Odense Kommune vedrørende kommunens påtænkte anvendelse af cloud computing i form af Google Apps,[115] i april 2011 foranlediget af en sikkerhedsbrist i forbindelse med Kommunernes Landsforenings (KL) overførsel af et køreprøve-bookingsystem til en cloud-løsning[116] og i 2012 vedrørende brug af en cloud-tjeneste i Office 365-pakken.[117] Ligeledes har det svenske datatilsyn i juni 2013 forholdt sig til offentlige myndigheders brug af Google Apps.[118]

I sagen vedrørende Odense Kommune angav Datatilsynet, at overførsel af oplysninger til datacentre i USA og visse lande i Europa, som ikke er medlemmer af EU, udgør en tredjelands-overførsel omfattet af persondataloven. En eventuel overførsel af oplysninger til datacentre i tredjelande forudsætter, at der er et lovligt grundlag for overførslen, for eksempel at der er indgået en aftale baseret på EU-Kommissionens standardkontrakt, og at der er søgt tilladelse fra Datatilsynet. Derudover skal det i aftalen med cloud-udbyderen fremgå, at denne udelukkende må handle efter instruks fra myndigheden, ligesom det skal fremgå, at sikkerhedsbekendtgørelsen gælder for databehandlingerne hos udbyderen.

Det skal godtgøres, at sikkerhedsbekendtgørelsens og persondatalovens krav vil blive opfyldt på en række punkter, herunder sletning af data, så de ikke kan genskabes, sikkerhed ved transmission og log-in, kontrol med afviste adgangsforsøg og logningskravet. Datatilsynet sætter blandt andet spørgsmålstegn ved, om persondatalovens krav om kontrol med sikkerhedsforanstaltningerne kan efterleves, når myndigheden ikke ved, hvor oplysningerne fysisk befinder sig. Datatilsynet anbefalede endvidere, at myndigheder benytter den tjekliste, som European Network and Information Security Agency (ENISA) har udarbejdet, i forhold til at risikovurdere cloud-tjenester.[119]

I forhold til overførsel til USA lagde Datatilsynet i den konkrete sag til grund, at den pågældende cloud-tjeneste (Google Inc.) har tilsluttet sig Safe Harbor-principperne, hvorfor overførsel af personoplysninger til disse datacentre vil kunne ske i overensstemmelse med persondataloven. Da safe harbor-ordningen nu er tilsidesat som ugyldig, må det antages, at cloud-tjenesterne fremover i stedet skal handle i overnesstemmelse med den nye Privacy Shield aftale.

Sagen rejser en række generelle spørgsmål i forhold til at sikre beskyttelsen af personoplysninger ved brug af cloud-tjenester, herunder hvorledes man sikrer, at underleverandører til cloud-tjenester lever op til såvel EU's standarder som til sikkerhedsbekendtgørelsens krav. Den stigende brug af cloud-tjenester aktualiserer behovet for mere systematisk konsekvensanalyse i forbindelse med it-baserede løsninger i den offentlige forvaltning. Samtidig er det ét ud af mange eksempler på de udfordringer, nye it-løsninger rejser i relation til privatliv og databeskyttelse. Den daværende IT- og Telestyrelse udgav i maj 2011 en vejledning om lovgivningskrav og kontraktmæssige forhold i forbindelse med cloud computing.[120] Vejledningen, der retter sig både mod offentlige myndigheder og private virksomheder, understreger blandt andet, at man inden kontraktindgåelse om en cloud-løsning skal gøre sig nøje overvejelser om, hvilke oplysninger der ønskes håndteret af cloud-leverandøren, således at der ikke opstår en situation, der må anses for at være i strid med den danske persondatalov eller sikkerhedsbekendtgørelsen.

5.4.3 ANBEFALINGER

Institut for Menneskerettigheder anbefaler – med henblik på at fremme menneskerettighederne – at Digitaliseringsstyrelsen:

- sikrer, at der opsamles erfaringer og udarbejdes guidelines og best practice-eksempler rettet mod offentlige myndigheders brug af cloud-tjenester, særligt vedrørende krav til sikkerhed og databeskyttelse.

5.5 EFTERRETNINGSTJENESTERNE OG CYBERSIKKERHED

Politiets Efterretningstjeneste (PET) er sammen med Forsvarets Efterretnings-tjeneste (FE) Danmarks sikkerhedstjeneste og udgør en del af det danske politi, hvis virksomhed i øvrigt er reguleret i politiloven.[121] PET's arbejde er baseret på indsamling af en stor mængde oplysninger om personer, organisationer, virksomheder mv. PET kan desuden anvende forskellige tvangsindgreb som aflytning, dataaflæsning, ransagning og beslaglæggelse.

PET's virksomhed har indtil 2014 ikke været reguleret ved lov, men alene været fastlagt i instrukser, retningslinjer mv. I sommeren 2013 blev der vedtaget en lov for PET's virksomhed, som trådte i kraft den 1. januar 2014.[122] Loven svarer i det

væsentlige til det lovudkast, som er indeholdt i betænkning 1529/2012 fra Udvalget vedrørende Politiets og Forsvarets Efterretningstjenester (PET-udvalget), der blev nedsat i 1998. Samtidig med at lovforslaget vedrørende PET blev fremsat, blev der tillige fremsat lovforslag vedrørende en styrkelse af Folketingets Kontroludvalg[123] og lovforslag vedrørende en lovregulering af FE.[124] Begge lovforslag blev vedtaget med ikrafttræden den 1. januar 2014.[125]

FE har til opgave at forebygge og modvirke trusler udefra mod Danmark og danske interesserer. Et område, som får øget opmærksomhed og ressourcer, er trusler i cyberspace. I december 2012 blev Center for Cybersikkerhed oprettet under FE til at varsle om og imødegå trusler på internettet samt til at varetage opgaven som national it-sikkerhedsmyndighed og netsikkerhedstjeneste. I 2016 er centret i øvrigt blev tildelt en række tilsynsbeføjelser over for udbydere af net og tjenester, herunder adgang til at gennemføre tilsynsbesøg uden retskendelse.[126] Oprettelsen af Center for Cybersikkerhed skete blandt andet ved, at ansvaret for den statslige varslingstjeneste GovCERT blev overført fra den daværende IT- og Telestyrelse til FE. Dette blev den 25. juni 2014 fulgt op af vedtagelsen af en ny lov om Center for Cybersikkerhed med ikrafttræden den 1. juli 2014.[127] Som led i den nye lov overgår tilsynsopgaven med centret til Tilsynet med Efterretnings-tjenesterne (PET-tilsynet).

Nærværende tema fokuserer på nogle af de menneskeretlige problemstillinger, som reguleringen af efterretningstjenesterne såvel som Center for Cyber-sikkerhed rejser i forhold til beskyttelse af retten til privatliv og demokratisk kontrol.

5.5.1 DEN MENNESKERETLIGE BESKYTTELSE

Offentlige myndigheders, herunder politiets og efterretningstjenesters, indsamling, registrering, behandling og opbevaring af personoplysninger mv. skal være i overensstemmelse med EMRK artikel 8, Europarådets konvention om databeskyttelse, TEUF samt EU-chartret. Som fortolkningsbidrag til Europarådets konvention har Europarådets Ministerkomité vedtaget en anbefaling om regulering af brugen af persondata i politisektoren. Denne indeholder blandt andet en række anbefalinger til medlemsstaterne om behandling af persondata.[128] EU's databeskyttelsesdirektiv finder ikke anvendelse for behandling af oplysninger, der vedrører den offentlige sikkerhed, forsvar, statens sikkerhed og statens aktiviteter på det strafferetlige område. Der er dog ikke noget til hinder for, at medlemsstater fastsætter tilsvarende regler på disse områder.

I en rammeafgørelse fra 2008 har EU desuden fastlagt nærmere betingelser for beskyttelse af personoplysninger i forbindelse med politisamarbejde og retligt

samarbejde i kriminalsager.[129] Disse bestemmelser er udmøntet i en bekendtgørelse, der fastsætter, at der i forbindelse med det politimæssige og strafferetlige samarbejde inden for EU alene vil kunne behandles følsomme personoplysninger, hvis det er strengt nødvendigt (og ikke som efter persondata-loven, hvis det er nødvendigt).[130] Bekendtgørelsen fastsætter også regler om den registreredes rettigheder, som går videre end den regulering, der følger af persondataloven, blandt andet om den registreredes ret til at kræve berigtigelse mv. af oplysninger, som udveksles i forbindelse med grænseoverskridende politisamarbejde eller retligt samarbejde inden for EU. Den nye databeskyttelses-pakke, indeholder udover databeskyttelsesforordningen også et direktiv om behandlingen af personoplysninger på det strafferetlige område.[131] Som nævnt ovenfor blev Rådet og Europa-Parlamentet i december 2015 enige om udkast til databeskyttelsespakken,[132] som blev formelt vedtaget i april 2016. EU behandler aktuelt også en forordning om et nyt retsgrundlag for Europol,[133] som fastsætter høje standarder for databeskyttelse. Det bemærkes, at dansk deltagelse i et overstatsligt Europol samarbejde, som følge af rets-forbeholdet, forudsætter en parallelaftale, og at der pågår forhandlinger herom.

FN's særlige rapportør på området for terrorbekæmpelse og menneskeret har udarbejdet en rapport til fremme og beskyttelse af menneskerettigheder og grundlæggende rettigheder på området for terrorbekæmpelse. Rapporten opstiller 10 områder for "god praksis" i forbindelse med den retlige og institutionelle ramme for efterretningstjenester og tilsynet med disse.[134] Det anbefales blandet andet, at ny lovgivning såvel som praksis er underlagt effektiv kontrol og tilsyn for at sikre overensstemmelse med menneskeretlige standarder, samt at potentielle ofre for krænkelser har effektiv adgang til at klage samt at få vurderet deres sag.

I december 2013 vedtog FN's Generalforsamling den første resolution om retten til privatliv i en digital tidsalder.[135] Heri fastslås, at retten til privatliv er under pres, og at staterne er forpligtede til at sikre, at national lovgivning, der hjemler overvågning, er i overensstemmelse med de menneskeretlige standarder på området. Som opfølgning på resolutionen iværksatte FN's Højkommissær for Menneskerettigheder i 2014 en høring om overvågningsrelateret lovgivning og tilsyn på tværs af FN's medlemsstater. Dette har resulteret i en række anbefalinger på området. Blandt andet understreger Højkommissæren, at efterretningstjenesternes vide adgang til at opsamle data fordrer effektive retssikkerhedsmæssige garantier og tilsyn (§ 27). Forholdet mellem bekæmpelse af terrorisme og beskyttelse af menneskerettigheder – her særligt de aktuelle udfordringer knyttet til digital overvågning og retten til privatliv – er ligeledes behandlet i en rapport fra FN's særlige rapportør på området for terror-bekæmpelse og menneskeret fra september 2014.[136] Rapporten konkluderer i

øvrigt (§ 18), at masseovervågning af digital kommunikation udgør en alvorlig trussel mod beskyttelsen af retten til privatliv – som en international anerkendt norm fastlagt i ICCPR artikel 17.[137]

5.5.2 DANSKE FORHOLD

REGULERINGEN AF PET

PET har blandt andet til opgave at forebygge, modvirke og efterforske eventuelle forbrydelser mod Danmarks selvstændighed og sikkerhed samt anden alvorlig kriminalitet, herunder organiseret kriminalitet. Herudover udarbejder PET trusselsvurderinger, bistår det øvrige politi, foretager sikkerhedsgodkendelser og forestår livvagtstjeneste.

I januar 2013 blev der indgået en bred politisk aftale om en styrket regulering af PET's virksomhed og den parlamentariske kontrol med PET. Aftalen vedrørte en ny lov for PET, herunder oprettelse af et nyt Tilsyn med Efterretningstjenesterne (PET-tilsynet) til afløsning af Wamberg-udvalget samt en styrkelse af Folketingets Kontroludvalg. Den nye PET-lov svarer i det væsentlige til det lovudkast, der blev sendt til høring i 2012, og hvor blandt andet Institut for Menneskerettigheder afgav høringssvar.[138] Loven blev vedtaget den 30. maj 2013 og trådte i kraft den 1. januar 2014. Reguleringen skal ses i sammenhæng med en lovændring til styrkelse af Folketingets Kontroludvalg.[139]

Institut for Menneskerettigheder har i høringsfasen blandt andet påpeget, at PET-loven primært fokuserer på PET's behandling af personoplysninger og mangler et tilsvarende fokus på andre områder af PET's virksomhed. Det samme gælder PET-tilsynet, som primært fører tilsyn med PET's behandling af person-oplysninger og ikke PET's arbejde i marken, herunder brugen af agenter.

PET-loven ændrer ikke ved PET's arbejdsopgaver, men fastsætter nye regler for PET's adgang til at indsamle, bearbejde, registrere og videregive person-oplysninger mv. De betingelser, der opstilles for PET's behandling af oplysninger, er baseret på persondatalovens standarder.[140] Loven svarer – som anført – i hovedtræk til PET-udvalgets lovudkast. Der er imidlertid visse afvigelser, herunder at lovens regler for behandling af personoplysninger gælder "enhver person", uanset om denne er hjemmehørende i Danmark. Dette fremgik ikke af det oprindelige forslag. Ligeledes indeholder loven nu en regulering af PET's behandling af oplysninger om juridiske personer, for eksempel foreninger og organisationer, samt regler om indsigt og videregivelse. Loven fasætter endvidere sletningsregler for oplysninger vedrørende både fysiske og juridiske personer. Endelig skal PET afgive en årlig redegørelse til justitsministeren om sin virksomhed. Redegørelsen offentliggøres.

Som også fastlagt i det oprindelige lovforslag lemper loven PET's adgang til at registrere personoplysninger i sager vedrørende terrorbekæmpelse. Hvor PET's registrering af personoplysninger tidligere var begrænset til det absolut påkrævede, vil der fremover kunne registreres personoplysninger med henblik på terrorbekæmpelse, hvis en registrering "må antages at have betydning" for PET's arbejde med terrorbekæmpelse. Der vil således ikke være samme strenge krav til behovet og begrundelsen for en registrering. Disse kriterier bygger blandt andet på de kriterier, som Folketinget, i forbindelse med terrorpakke II, fastsatte for visse former for behandling af personoplysninger hos PET (retsplejelovens § 116).

Efter loven gælder et forbud mod registrering alene på grundlag af lovlig politisk virksomhed. Dette forbud gælder dog ikke undtagelsesfrit. PET vil – som hidtil – kunne behandle oplysninger om en persons politiske virksomhed med henblik på at afklare, om der er tale om lovlig virksomhed. PET vil også fortsat – ved behandlingen af oplysninger om politiske foreninger og organisationer – kunne medtage oplysninger om, hvem der udgør dennes ledelse. PET får derfor med loven en udtrykkelig ret til at registrere oplysninger om en persons politiske virksomhed, indtil det er afklaret, om virksomheden er lovlig. Viser undersøgelserne, at virksomheden er lovlig, skal personoplysningerne slettes. Forbuddet gælder ikke i forhold til fysiske personer, der ikke er hjemmehørende i Danmark, og forbuddet gælder – ligesom efter regeringserklæringen fra 1968 – ikke juridiske personer.

Derudover indeholder loven ikke noget forbud mod registrering af personer alene på baggrund af for eksempel deres religiøse overbevisning, ligesom der ikke fastsættes en særskilt ramme for PET's adgang til at behandle oplysninger om andre personer, der rammes af indgrebet (såkaldte bipersoner)**.**

PET-tilsynet består efter loven af fem medlemmer, der udpeges af justits-ministeren efter drøftelse med Kontroludvalget (formanden udpeges dog af landsretternes præsidenter). Mens Wamberg-udvalgets kontrol primært skete ved **forudgående godkendelser** af for eksempel registrering af person-oplysninger, består PET-tilsynets beføjelser i en **efterfølgende kontrol**. PET-tilsynet vil således først efterfølgende, af egen drift eller efter klage fra en borger, stikprøvevist eller i konkrete sager, kunne prøve PET's registreringer. Tilsynet kan i øvrigt ikke påbyde PET bestemte foranstaltninger i forhold til behandlingen af oplysninger, men kan alene afgive udtalelser, herunder kritik, henstillinger og sin opfattelse af en sag. Disse udtalelser er ikke retligt bindende, men PET-loven forudsætter, at PET-loven og dennes forarbejder, at PET i almindelighed følger dem.

Efter loven har en person ikke ret til indsigt i oplysninger, som PET behandler om vedkommende, eller ret til at få oplyst, om PET overhovedet behandler sådanne oplysninger. Vedkommende kan dog anmode PET-tilsynet om at undersøge, om PET uberettiget behandler oplysninger om vedkommende. Tilsynet kan i så fald bindende pålægge PET at slette oplysningerne og i særlige tilfælde at give indsigt i oplysningerne. Denne ordning omfatter også fysiske personer og juridiske personer, der ikke er hjemmehørende i Danmark.

Styrkelsen af Folketingets Kontroludvalg består i, at regeringen har pligt til at give udvalget en årlig orientering om PET's virksomhed, herunder brugen af civile agenter. PET skal også orientere udvalget om sager, hvor PET har foretaget tvangsindgreb, som domstolene ikke har godkendt. Instituttet bemærkede i sit høringssvar, at de nye regler alene indeholder en styrkelse af den orientering, som Kontroludvalget modtager, men udvalget er fortsat ikke er blevet tildelt en selvstændig kontrolfunktion,[141] og det vil fortsat være afhængigt af de informationer, som det modtager fra PET.

Som nævnt ovenfor har instituttet også fremhævet, at den nye regulering på området vægter PET's behandling af personoplysninger, men kun i begrænset omfang indeholder regler om PET's politimæssige arbejde, herunder brugen af agenter. Reguleringen og kontrollen med PET vil således være begrænset til bestemte områder for PET's virksomhed og vil efter instituttets opfattelse ikke leve op til internationale anbefalinger for en uafhængig og effektiv kontrol med efterretningstjenesterne i et moderne retssamfund.[142]

Justitsministeriet har i sine bemærkninger til instituttets anbefalinger i status 2013 bemærket, at PET udover kontrol fra PET-tilsynet og Kontroludvalget, også er underlagt kontrol fra blandt andet domstolene og Folketingets Ombudsmand, hvorfor der efter ministeriets opfattelse ikke behov for at etablere yderligere kontrol med PET.

Domstolskontrollen er dog i civile sager væsentligt begrænset af retsplejelovens editions- og vidnebeskyttelsesregler, og PET kan som hovedregel nægte at udlevere tavshedsbelagte oplysninger til brug for sager ved domstolene. Hertil kommer, at domstolenes kontrol med forvaltningen, herunder PET, i sit udgangspunkt er en legalitetskontrol, og domstolene prøver således ikke forvaltningens skøn.[143] Ombudsmanden har ikke samme begrænsninger i sin adgang til oplysninger,[144] hvilket kunne være en fordel på netop dette område. Uanset at forvaltningmyndighederne almindeligvis følger Ombudsmandens kritik mv., har heller ikke Ombudsmanden beføjelse til med bindende virkning at

pålægge PET at handle på en given måde, hvilket instituttet ser som et af de væsentlige problemer med PET-tilsynet.

FE OG CENTER FOR CYBERSIKKERHED

FE er – udover Danmarsk udenrigs- og militære efterretningstjeneste – også national it-sikkerhedsmyndighed, militær (MILCERT) og statslig (GovCERT) varslingstjeneste for internettrusler. Tilsynet med FE varetages, ligesom tilsynet med PET, af Tilsynet med Efterretningstjenesterne (PET-tilsynet) og Folketingets Kontroludvalg. Tilsynet svarer i det store hele til tilsynet med PET, dog således at klageadgangen alene tilkommer i Danmark hjemmehørende fysiske og juridiske personer, og vil derfor ikke blive behandlet yderligere i det følgende.[145]

Som led i regeringsgrundlaget i 2011 blev det besluttet at nedlægge IT- og Telestyrelsen og samtidig flytte ressortansvaret for sager vedrørende beskyttelse af kritisk it-infrastruktur samt statens varslingstjeneste for internettrusler (GovCERT) til Forsvarsministeriet.[146] På denne baggrund blev Center for Cybersikkerhed den 18. december 2012 oprettet under FE til at varetage opgaven som national it-sikkerhedsmyndighed (PET varetager denne funktion på Justitsministeriets område) samt varslingstjenesterne MILCERT og GovCERT.

Med oprettelsen af Center for Cybersikkerhed blev GovCERT de facto en del af FE, mens der først i februar 2014 blev fremsat forslag til lov om Center for Cybersikkerhed.

Lovforslaget blev kritiseret af flere høringsparter, herunder Institut for Menneskerettigheder, som blandt andet påpegede, at placeringen af GovCERT under Center for Cybersikkerhed medfører, at tjenesten (modsat da GovCERT hørte under IT- og Telestyrelsen) undtages fra offentlighedsloven, forvaltningsloven og persondataloven, herunder Datatilsynets tilsynsvirksomhed.[147]

Tilsynet med Center for Cybersikkerheds behandling af personoplysninger varetages af PET-tilsynet, hvis beføjelser i denne henseende svarer til tilsynets beføjelser i relation til PET og FE, dog således at der i medfør af loven om Center for Cybersikkerhed end ikke gælder en indirekte indsigts-ordning. Samtidig blev GovCERTs grundlag for dataindsamling udvidet, idet kredsen af virksomheder, der kan tilslutte sig GovCERT, blev udvidet fra virksomheder, der er beskæftiget med kritisk infrastruktur, til en bredere gruppe af virksomheder beskæftiget med samfundsvigtige funktioner.

Placeringen af GovCERT i Center for Cybersikkerhed, under FE, medfører endvidere, at der nu som udgangspunkt er fri adgang til at udveksle data mellem GovCERT og den øvrige del af FE i medfør af almindelige forvaltningsretlige

principper. Hertil kommer en vid adgang for udveksling af oplysninger efterretningstjenesterne imellem. Som en konsekvens af, at persondataloven ikke gælder for Center for Cybersikkerhed, har Forsvarsministeriet udstedt retningslinjer for behandling af personoplysninger mv.[148] Nogle af persondatalovens principper er herudover indskrevet i lov om Center for Cybersikkerhed. De administrative retningslinjer skal blandt andet sikre, at intern udveksling af oplysninger mellem Center for Cybersikkerhed og den øvrige efterretningstjeneste sker med respekt for retssikkerheden og den personlige frihed. Instituttet påpegede i sit høringssvar, at det er betænkeligt, at dette ikke sikres på lovniveau. Data, som centret er i besiddelse af som statslig varslingstjeneste for danske myndigheder og en lang række private virksomheder, vil således kunne inddrages i FE's øvrige arbejde inden for det militære område.

Ligeledes blev det i flere høringssvar fremhævet, at centrets mulighed for ekstern videregivelse af data er for vidtgående. Ved begrundet mistanke om en sikkerhedshændelse kan både indholds- og trafikdata videregives til politiet. Trafikdata kan desuden videregives til blandt andet danske myndigheder og udenlandske netsikkerhedstjenester, hvis det vurderes nødvendigt for udførelsen af netsikkerhedstjenestens opgaver. Derudover blev der rejst kritiske spørgsmål i forhold til PET-tilsynets mandat og kompetence, herunder manglende teknisk sagkundskab.

De mange kritiske høringssvar medførte en del offentlig debat og et møde i Forsvarsministeriet, hvor høringsparterne blev inviteret til en drøftelse af lovforslaget. Høringsfasen medførte enkelte, men centrale ændringer, særligt en skærpet ordlyd i bestemmelsen om videregivelse af data (lovens § 16), således at videregivelse kræver "en begrundet mistanke om en sikkerhedshændelse" og ikke blot, at det "vurderes nødvendigt for udførelsen af netsikkerhedstjenestens opgaver".

Med vedtagelsen af lov om net- og informationssikkerhed blev Center for Cybersikkerhed i 2015 herudover tillagt en række tilsynsbeføjelser over for udbydere af net og tjenester, herunder adgang til at gennemføre tilsynsbesøg uden retskendelse.[149] Instituttet rejste i sit høringssvar spørgsmålstegn ved, om det fortsat er berettiget at undtage centret fra de forvaltningsretlige krav, der stilles til andre tilsynsmyndigheder.[150]

Afslutningsvis skal det bemærkes, at FE-loven er blevet ændret i 2015, så det nu er muligt for FE at indsamle oplysninger om danske borgere, når de befinder sig i udlandet, såfremt der er bestemte grunde til at formode, at vedkommende deltagere i aktiviteter, der kan indebære eller forøge en terrortrussel mod Danmark.[151] FE kunne også forinden indsamle alle former for oplysninger, så længe indsamlingen var rettet mod udlandet, og videregive data fra overvågning til andre efterretningstjenester, men danske borgere har hidtil været beskyttet

mod sådanne tiltag, da FE ikke har kunnet behandle oplysninger om danske borgere, med mindre dette skete ved et tilfælde. Lovforslaget blev mødt med kritik fra blandt andre Institut for Menneskerettigheder, der påpegede, at mistankekravet var lavere end efter de almindelige regler i strafferetsplejen, og som ligeledes beskrevet ovenfor, at FE er underlagt et mangelfuldt tilsyn.[152] Der henvises i øvrigt til delrapporten om retfærdig rettergang, afsnit 5.3. om indgreb i meddelelseshemmeligheden.

5.5.3 ANBEFALINGER

Institut for Menneskerettigheder anbefaler – med henblik på at fremme den enkeltes menneskerettigheder – at regeringen:

- foretager en kortlægning og systematisk vurdering af det samlede tilsyn med efterretningstjenesterne, herunder Center for Cybersikkerhed.

- udvider PET-tilsynets kompetence til hele PET's virksomhed, samt giver tilsynet beføjelse til at kunne påbyde efterretningstjenesterne bestemte foranstaltninger i forhold til behandlingen af oplysninger.

- udvider adgangen til indsigt i efterretningstjenesternes virksomhed for den enkelte fysiske eller juridiske person.

SLUTNOTER

[1] Office of the Privacy Commissioner of Canada, "Privacy Impact Assessments", december 2011, tilgængelig på: www.priv.gc.ca/fs-fi/02_05_d_33_e.cfm.
[2] FN's Verdenserklæring om Menneskerettighedernes artikel 12.
[3] ICCPR's artikel 17, Børnekonventionens artikel 16 og Handicapkonventionens artikel 22.
[4] The right to privacy in the digital age, Resolution 28/16 adopted by the Human Rights Council on 1 April 2015. A/HRC/RES/28/16.
5 Europarådets konvention om beskyttelse af det enkelte menneske i forbindelse med elektronisk databehandling af personoplysningers artikel 5.
[6] Retsudvalget, Alm. del 2015-16 – bilag 134, 'Notat om status på forhandlinger på Justitsministeriets område om indgåelse af internationale aftaler uden for EU-området´, tilgængelig på: www.ft.dk/samling/20151/almdel/reu/bilag/134/1590969.pdf.
[7] EU-chartrets artikel 8.
[8] Europa-Parlamentet og Rådets direktiv 95/46/EF af 24. oktober 1995 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger.
[9] Rådets rammeafgørelse af 27. november 2008 om beskyttelse af personoplysninger i forbindelse med politisamarbejde og retligt samarbejde i kriminalsager, 2008/977/RIA.
[10] Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, COM(2010) 609 final, 4. november 2011, tilgængelig på: http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_en.pdf.
[11] Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (generel forordning om databeskyttelse), tilgængelig på http://eur-lex.europa.eu/legal-content/DA/TXT/HTML/?uri=CELEX:32016R0679&from=EN.
[12] 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 og om ophævelse af

Rådets rammeafgørelse 2008/977/RIA, tilgængelig på http://eur-lex.europa.eu/legal-content/DA/TXT/HTML/?uri=CELEX:32016L0680&from=EN.
[13] Se mere på Europa-Kommissionens hjemmeside, http://ec.europa.eu/justice/data-protection/
[14] Grundlovens §§ 71 og 72.
[15] Grundlovens § 72.
[16] Bekendtgørelse nr. 528 af 15. juni 2000.
[17] Datatilsynets Årsrapport 2014, side 6.
[18] The Right to Privacy in the Digital Age, Resolution adopted by the General Assembly on 18 December 2013. A/RES/68/167. The Right to Privacy in the Digital Age, Resolution adopted by the General Assembly on 18 December 2014. A/RES/69/166.
[19] The Right to Privacy in the Digital Age, Report of the Office of the United Nations High Commissioner for Human Rights, 30. juni 2014. A/HR/C/27/37.
[20] The Right to Privacy in the Digital Age, Resolution adopted by the Human Rights Council on 1 April 2015. A/HRC/RES/28/16.
[21] EU-Domstolens dom af 6. oktober 2015 i sag C-362/14, Maximilian Schrems mod Data Protection Commissioner og Digital Rights Ireland Ltd.
[22] Kommissionen, 'EU Commission and United States agree on new framework for transatlantic data flows: EU-US Privacy Shield', press release, 2. februar 2016, tilgængelig på: http://europa.eu/rapid/press-release_IP-16-216_en.htm.
[23] Europa Parlamentet, 'Data protection package: Parliament and Council now close to a deal', press release, 15. December 2015, tilgængelig på: www.europarl.europa.eu/news/en/news-room/20151215IPR07597/Data-protection-package-Parliament-and-Council-now-close-to-a-deal.
[24] Lov nr. 652 af 18. maj 2015 om ændring af arkivloven (Særlig regulering i arkivloven af Dansk AlmenMedicinsk Database (DAMD)).
[25] Office of the United Nations High Commissioner for Human Rights, Special Rapporteur on the right to privacy, tilgængelig på: www.ohchr.org/EN/Issues/Privacy/SR/Pages/SRPrivacyIndex.aspx.
[26] Se blandt andet Institut for Menneskerettigheder, 'Høring over udkast til lov om ændring af lov om politiets efterretningstjeneste og toldloven (Politiets Efterretningstjenestes adgang til oplysninger om flypassagerer i terrorsager og SKAT's håndtering af oplysninger om flypassagerer i forbindelse med toldkontrol', 6. maj 2015, tilgængelig på: http://menneskeret.dk/sites/menneskeret.dk/files/05_maj_15/57_b_pet_skat_oplysninger_flypassagerer.pdf.
[27] Lov nr. 1881 af 29. december 2015 om ændring af lov om Politiets Efterretningstjeneste (PET) og toldloven.
[28] Lov nr. 1571 af 15. december 2015 om ændring af lov om Forsvarets Efterretningstjeneste (Styrket indsats mod aktiviteter i udlandet, der kan indebære en terrortrussel mod Danmark og danske interesser).

[29] Institut for Menneskerettigheder, 'Høring over udkast til lov om ændring af lom om Forsvarets Efterretningstjeneste', 4. maj 2015.
[30] Data Retention Directive 2006/24/EC af 31. maj 2011.
[31] Justitsministeriets notat af 2. juni 2014 om betydningen af EU-Domstolens dom af 8. april 2014 i de forenede sager C-293/12 og C-594/12 (om logningsdirektivet) for de danske logningsregler, tilgængelig på: http://justitsministeriet.dk/sites/default/files/media/Pressemeddelelser/pdf/2014/Notat%20om%20logningsdirektivet.pdf.
[32] Bekendtgørelse nr. 660 af 19. juni 2014 om ændring af bekendtgørelse om udbydere af elektroniske kommunikationsnets og elektroniske kommunikationstjenesters registrering og opbevaring af oplysninger om teletrafik (logningsbekendtgørelsen).
[33] Det varslede forslag er blandt andet blevet beskrevet i Advokatsamfundet, "Appel til Justitsministeren: Udsæt revision af sessionslogningsregler", 11. februar 2016, tilgængelig på: www.advokatsamfundet.dk/Service/Nyheder/2016/Justitsminister%20sessionslogning.aspx.
[34] DR, "Justitsministeren sparker forslag om internetovervågning til til hjørne", 17. marts 2016.
[35] Se Berlingske, den 30. oktober 2015, tilgængelig på link: www.b.dk/nationalt/regeringen-nedlaegger-uvildigt-terror-udvalg.
[36] Folketingets Retsudvalg og Kulturudvalg, Beretning nr. 3 af 3. juni 2014 om nedsættelse af en parlamentarisk arbejdsgruppe, der skal undersøge mulighederne for en bedre beskyttelse af personfølsomme oplysninger og et effektivt tilsyn med offentlige institutioner såvel som private virksomheders behandling af disse.
[37] For en status på arbejdsgruppens arbejde se: www.ft.dk/Folketinget/udvalg_delegationer_kommissioner/Udvalg/Retsudvalget/Nyheder/2014/10/Statusnyhed_arbejdsgruppe_REU.aspx.
[38] Lov nr. 1567 af 15. december 2015 om net- og informationssikkerhed.
[39] Institut for Menneskerettigheder, Høring over forslag til lov om net- og informationssikkerhed, 7. maj 2015.
[40] Opinion of the European Data Protection Supervisor (EDPS) on the Evaluation report from the Commission to the Council and the European Parliament on the Data Retention Directive (Directive 2006/24/EC), 31. maj 2011.
[41] EDPS on the proposal for a Directive of the European Parliament and of the Council on the retention of data processed in connection with the provision of public electronic communication services and amending Directive ((2002/58/EC(COM(2005) 438 final), 2005/C 298/01, 26. september 2005.
[42] Peter Hustinx, EDPS, "The moment of truth for the Data Retention Directive", speech, Bruxelles, 3. december 2010.

[43] Brev af 22. juni 2010 fra en række organisationer til kommissær Malmström, Reding and Kroes, tilgængelig på: www.vorratsdatenspeicherung.de/images/DRletter_Malmstroem.pdf.
[44] Article 29 Working Party, Opinion 3/2006.
[45] Frank La Rue, "Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression", UN Human Rights Council, A/HRC/23/40, 17. april 2013.
[46] Afgørelse fra EU-Domstolen, 14. april 2014, tilgængelig på: http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054en.pdf.
[47] Lov nr. 378 af 6. juni 2002 om ændring af straffeloven, retsplejeloven, lov om konkurrence- og forbrugerforhold på telemarkedet, våbenloven, udleveringsloven samt lov om udlevering af lovovertrædere til Finland, Island, Norge og Sverige.
[48] Retsplejelovens § 786, stk. 4.
[49] Bekendtgørelse nr. 988 af 28. september 2006 om udbydere af elektroniske kommunikationsnets og elektroniske kommunikationstjenesters registrering og opbevaring af oplysninger om teletrafik (logningsbekendtgørelsen).
[50] Oversigt over høringssvar, Justitsministeriet, 14. december 2011, tilgængelig på: http://webarkiv.ft.dk/img20012/udvbilag/lib9/20012_1119.pdf.
[51] Europa-Parlamentets og Rådets direktiv 2006/24/EF af 15. marts 2006 om lagring af data genereret eller behandlet i forbindelse med tilvejebringelse af offentligt tilgængelige elektroniske kommunikationstjenester eller elektroniske kommunikationsnet og om ændring af direktiv 2002/58/EF.
[52] http://jurist.org/paperchase/2012/12/austria-court-finds-eu-data-retention-plan-violates-eu-privacy-law.php.
[53] EU-Kommissionens evalueringsrapport fra 18. april 2011; COM(2011) 225 final.
[54] EU-Domstolens dom af 30. maj 2013 i sag C‑270/11, Kommissionen mod Sverige.
[55] EU-Domstolens dom af 8. april 2014 i de forenede sager C-293/12 og C-594/12.
[56] Retsudvalget 2015-2016, 'Notat til Folketingets Europaudvalg om afgivelse af indlæg i EU-Domstolens sag C-698/15, Davis m.fl.', tilgængelig på: www.ft.dk/samling/20151/almdel/reu/bilag/192/1603777.pdf.
[57] Udkast til forslag til lov om ændring af lov om ændring af straffeloven, retsplejeloven, lov om konkurrence- og forbrugerforhold på telemarkedet, våbenloven, udleveringsloven samt lov om udlevering af lovovertrædere til Finland, Island, Norge og Sverige (Ophævelse af revisionsbestemmelse), 17. februar 2010.
[58] Telekommunikationsindustriens høringssvar af 25. november 2011 om ændring af revisionsbestemmelsen.
[59] Version2, 'Nu stopper sessionslogning: Massesletning af data begynder', 18. juni 2014.

[60] Justitsministeriets notat om betydningen af EU-Domstolens dom af 8. april 2014 i de forenede sager C-293/12 og C-594/12 (om logningsdirektivet) for de danske logningsregler af 2. juni 2014, tilgængelig på: http://justitsministeriet.dk/sites/default/files/media/Pressemeddelelser/pdf/2014/Notat%20om%20logningsdirektivet.pdf.
[61] Bekendtgørelse nr. 660 af 19. juni 2014.
[62] Berlingske, "Politiet vil genindføre overvågning af danskere på internettet", 7. januar 2014, tilgængelig på: www.b.dk/nationalt/politiet-vil-genindfoere-overvaagning-af-danskere-paa-internettet.
[63] Regeringen, 'Lovgivning Folketingsåret 2015/2016', oktober 2015.
[64] Det varslede forslag er blandt andet blevet beskrevet i Advokatsamfundet, "Appel til Justitsministeren: Udsæt revision af sessionslogningsregler", 11. februar 2016, tilgængelig på: www.advokatsamfundet.dk/Service/Nyheder/2016/Justitsminister%20sessionslogning.aspx.
[65] Der henvises blandt andet til debatten om logning på Altinget, herunder Jesper Lunds inlæg, 'IT-forening: Brug for uafhængig evaluering af logningsregler', 28. januar 2016, og Rikke Frank Jørgensens indlæg 'IMR: Hold fast i kravet om evaluering af logningsregler', 4. februar 2016 og Retsudvalget, Samrådsspørgsmål AS-AY, Folketingssamlingen 2015-16.
[66] Altinget, 'IMR: Vent med at indføre nye logningsregler', Rikke Frank Jørgensen, 21. januar 2016, og 'IMR: Hold fast i kravet om evaluering af logningsregler', Rikke Frank Jørgensen, 4. februar 2016.
[67] DR, "Justitsministeren sparker forslag om internetovervågning til til hjørne", 17. marts 2016.
[68] Lov nr. 1881 af 29. december 2015 om ændring af lov om Politiets Efterretningstjeneste (PET) og toldloven.
[69] Lov nr. 1571 af 15. december 2015 om ændring af lov om Forsvarets Efterretningstjeneste (Styrket indsats mod aktiviteter i udlandet, der kan indebære en terrortrussel mod Danmark og danske interesser).
[70] Bekendtgørelse nr. 1776 af 16. december 2015 om politiets anvendelse af automatisk nummerpladegenkendelse (ANPG).
[71] UN Human Rights Council, 'Draft Report of the Working Group on the Universal Periodic Review', 25 January 2016, A/HRC/WG.6/24/L.7.
[72] Article 29 Working Party: Opinion 5/2009.
[73] EC justice, Reform of data protection legislation, 6. februar 2011, tilgængelig på: http://ec.europa.eu/justice/data-protection/index_en.htm.
[74] Europarådet, "Recommendation CM/Rec(2012)4 of the Committee of Ministers to Member States on the Protection of Human Rights with Regard to Social Networking Services", 4. april 2012.
[75] Institut for Menneskerettigheder, DR, Berlingske Media, Forbrugerrådet og Medierådet for Børn og Unge, "Teenagere, deres private og offentlige liv på de

sociale medier", online-survey, februar 2013, tilgængelig på: http://issuu.com/dkmediacouncil/docs/teenagere_deres_private_og_offentlige_liv_p__socia.

[76] Tænketanken Digitale Unge, november 2013. Fokusgruppe-undersøgelsen: Unges Private og Offentlige liv på Sociale Medier.

[77] Vejledningen om ansvar og ret på sociale medier er tilgængelig på: http://digitaleunge.dk/2014/05/12/faq-om-ret-og-ansvar-pa-sociale-medier/#more-779.

[78] Datatilsynet, "Nordiske Datatilsyn ønsker klarhed om Facebooks håndtering af personoplysninger", 8. juli 2011.

[79] Facebook's Response to Questions from the Data Inspectorate of Norway, september 2011, tilgængelig på: www.datatilsynet.no/Global/english/Facebook_questions_answere2011.pdf.

[80] Pressemeddelse fra Datatilsynet i Slesvig-Holsten den 15. februar 2013, tilgængelig på: www.datenschutzzentrum.de/presse/20130215-verwaltungsgericht-facebook.htm.

[81] The Irish Data Protection Commissioner, "Final Report of audit of Facebook Ireland", december 2011, tilgængelig på: www.dataprotection.ie/docs/Facebook-Ireland-Audit-Report-December-2011/1187.htm.

[82] Europe v. Facebook, tilgængelig på: http://europe-v-facebook.org/EN/en.html.

[83] EU-Domstolens dom af 6. oktober 2015 i sag C-362/14, Maximilian Schrems.

[84] The Federal Trade Commission, "Facebook Settles FTC Charges That It Deceived Consumers By Failing To Keep Privacy Promises", 29. november 2011, tilgængelig på: www.ftc.gov/opa/2011/11/privacysettlement.shtm.

[85] Datatilsynet, "Persondataloven og Sociale Netværk", 2. november 2008, tilgængelig på: www.datatilsynet.dk/borger/sociale-netvaerk/persondataloven-og-sociale-netvaerk.

[86] Folketingets Ombudsmand, "Myndigheder må bruge oplysninger fra åbne Facebook-profiler", sagsnummer 2011 15-1, 15. januar 2011.

[87] Tilgængelig på www.europarl.europa.eu/europa-huset/view/da/set_og_sket/set_og_sket_2013/internetcencur.html;jsessionid=B834AF52C961379666D389D9647D52F4.

[88] Tilgængelig på: www.ft.dk/Folketinget/udvalg_delegationer_kommissioner/Udvalg/Kulturudvalget/Nyheder/2014/02/Hoering_censur_beskyttelse_data.aspx.

[89] Medierådet for Børn og Unge i samarbejde med Forbrugerrådet Tænk, Institut for Menneskerettigheder, Digital Identitet, Danish Science Factory og Børnerådet, 'Din guide til menneskerettigheder på internettet', 2014.

[90] The Right to Privacy in the Digital Age, Resolution adopted by the General Assembly on 18 December 2013. A/RES/68/167.

[91] Report of the Office of the High Commissioner for Human Rights, "The Right to Privacy in the Digital Age", A/HR/C/27/37, 30. juni 2014.
[92] The Right to Privacy in the Digital Age, Resolution adopted by the General Assembly on 19 November 2014. A/C.3/69/L.26/Rev.1.
[93] Datatilsynet, 'Uvedkommendes adgang til personoplysninger i systemer, som Rigspolitiet er ansvarlig for', afgørelse af 31. juli 2015.
[94] Rigsrevisionen beretning fra november 2013 er tilgængelig på: www.rigsrevisionen.dk/media/1943109/rs-2012.pdf.
[95] Rigsrevisionen beretning fra november 2014 er tilgængelig på: http://www.rigsrevisionen.dk/media/2011989/statens-behandling-af-fortrolige-oplysninger-om-personer-og-virksomheder.pdf.
[96] Rigsrevisionen, 'Beretning til Statsrevisorerne om adgangen til it-systemer, der understøtter samfundsmæssige opgaver', oktober 2015.
[97] Beretning nr. 3 afgivet den 3. juni 2014 af Kulturudvalget og Retsudvalget om nedsættelse af en parlamentarisk arbejdsgruppe, der skal undersøge mulighederne for en bedre beskyttelse af personfølsomme oplysninger og et effektivt tilsyn med offentlige institutioner såvel som private virksomheders behandling af disse.
[98] Bekendtgørelse nr. 528 af 15. juni 2000 om sikkerhedsforanstaltninger til beskyttelse af personoplysninger, som behandles for den offentlige forvaltning.
[99] Oplæg fra Lena Andersen, Datatilsynet, ved høring i retsudvalget den 23. oktober 2014, tilgængelig på: www.ft.dk/webtv/video/20131/reu/tv.2453.aspx?as=1.
[100] Materiale fra arbejdsgruppens arbejde er tilgængelig på: www.ft.dk/Folketinget/udvalg_delegationer_kommissioner/Udvalg/Retsudvalget/Nyheder/2014/10/Statusnyhed_arbejdsgruppe_REU.aspx
[101] Institut for Menneskerettigheders høringssvar af 2. juli 2012 om Generel forordning om databeskyttelse.
[102] http://europa.eu/rapid/press-release_MEMO-14-186_da.htm.
[103] Europa Parlamentet, 'Data protection package: Parliament and Council now close to a deal', press release, 15. December 2015, tilgængelig på: www.europarl.europa.eu/news/en/news-room/20151215IPR07597/Data-protection-package-Parliament-and-Council-now-close-to-a-deal.
[104] Teknologirådet, "Retssikkerhed og aktivt medborgerskab i digital forvaltning", 2005/13.
[105] Dansk Industri/ITEK, "God Privacy Praksis – en guideline for IT-leverandør og kunder", 2007.
[106] Digitaliseringsstyrelsen, "Guide til konsekvensvurdering af privatlivsbeskyttelse", maj 2013.
[107] Digitaliseringsstyrelsen, "Vejledning i vurdering af offentlige it-projekters potentielle konsekvenser for privatlivet", maj 2013.

[108] Vejledningen er tilgængelig på: http://di.dk/Virksomhed/Produktion/IT/Informations-sikkerhed%20og%20Privacy/Trusler%20og%20loesninger/Pages/DIsskabelonforPrivacyImpactAssessment.aspx.
[109] Article 29 Working Party: Opinion 05/2012, side 5.
[110] Article 29 Working Party: Opinion 05/2012, side 5.
[111] Domstolens dom af 6. oktober 2015 i sag C-362/14, Maximilian Schrems.
[112] European Commission, 'Restoring trust in transatlantic data flows through strong safeguards: European Commission presents EU-U.S. Privacy Shield' press release, 29. Februar 2016, tilgængelig på: http://europa.eu/rapid/press-release_IP-16-433_en.htm.
[113] Maximilian Schrems, 'EU US Privacy Shield" (Safe Harbor 1.1) "European Commission may be issuing a round-trip to Luxembourg', tilgængelig på http://europe-v-facebook.org/PS_update.pdf.
[114] It-sikkerhedskomitéen, "Sikkerhed i Cloud Computing," december 2010.
[115] Datatilsynet, "Behandling af følsomme personoplysninger i cloud-løsning", 3. februar 2011.
[116] Datatilsynet, brev vedrørende "sikkerhedsbrist som følge af KL's overførsel af køreprøvebookingsystem til en cloud-løsning", 15. april 2011, tilgængelig på: www.datatilsynet.dk/fileadmin/user_upload/dokumenter/Breve/Brev_til_KL_om_sikkerhedsbrist_ved_brug_af_cloud.pdf.
[117] Datatilsynet, "Behandling af personoplysninger i cloud-løsningen Office 365", 6. juni 2012.
[118] Datainspektionen, afgørelse af 31. maj 2013, sagsnummer 1351-2012, tilgængelig på: www.datainspektionen.se/Documents/beslut/2013-05-31-salems-kommun.pdf.
[119] ENISA, "Cloud Computing – Benefits, risks and recommendations for informations security", november 2009, tilgængelig på: www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment/at_download/fullReport.
[120] IT- og Telestyrelsen "Cloud computing og de juridiske rammer – En vejledning om lovgivningskrav og kontraktmæssige forhold i forbindelse med cloud computing", maj 2011.
[121] Lov nr. 444 af 9. juni 2004 om politiets virksomhed.
[122] Lov nr. 604 af 12. juni 2013 om politiets efterretningstjeneste (PET).
[123] Forslag nr. 162 af 27. februar 2013 til lov om ændring af lov om etablering af et udvalg om forsvarets og politiets efterretningstjenester.
[124] Forslag nr. 163 af 27. februar 2013 til lov om Forsvarets Efterretningstjeneste (FE).
[125] Se henholdsvis lov nr. 632 af 12. juni 2013 om ændring af lov om etablering af et udvalg om forsvarets og politiets efterretningstjenester og lov nr. 602 af 12. juni 2013 om Forsvarets Efterretningstjeneste (FE).

[126] Lov nr. 1567 af 15. december 2015 om net- og informationssikkerhed.
[127] Lov nr. 713 af 25. juni 2014 om Center for Cybersikkerhed.
[128] Recommandation of The Committee of Ministers to Member States "Regulating the Use of Personal Data in the Police Sector", recommandation no. R (87) 15.
[129] Rådets rammeafgørelse af 27. november 2008 om beskyttelse af personoplysninger i forbindelse med politisamarbejde og retligt samarbejde i kriminalsager, 2008/977/RIA.
[130] Bekendtgørelse nr. 1287 af 25. november 2010.
[131] Proposal for a Directive of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data by Competent Authorities for the Purposes of Prevention, Investigation, Detection or Prosecution of Criminal Offences or the Execution of Criminal Penalties, and the Free Movement of Such Data, COM(2012) 10 final, 2012. Se i den forbindelse Institut for Menneskerettigheders høringssvar af 1. oktober 2012.
[132] Europa Parlamentet, 'Data protection package: Parliament and Council now close to a deal', press release, 15. December 2015, tilgængelig på: www.europarl.europa.eu/news/en/news-room/20151215IPR07597/Data-protection-package-Parliament-and-Council-now-close-to-a-deal.
[133] Se Institut for Menneskerettigheders høringssvar af 11. juli 2013.
[134] Martin Scheinin, "Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism", A/HRC/16/51/Add.1, 22. december 2010.
[135] The Right to Privacy in the Digital Age, Resolution adopted by the General Assembly on 18 December 2013. A/RES/68/167.
[136] Ben Emmerson, "Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism", 23. september 2014. A/69/397.
[137] The Right to Privacy in the Digital age, Report of the Office of the United Nations High Commissioner for Human Rights, 30. juni 2014. A/HR/C/27/37.
[138] Oversigt over høringssvar vedrørende betænkning om PET. Tilgængelig på: http://menneskeret.dk/files/images/PET%20billeder/PET%20doks/Høringssvar%20vedr%20%20PET-betænkning.pdf.
[139] Lov nr. 632 af 12. juni 2013 om styrkelse af kontroludvalgets beføjelser.
[140] Lov nr. 429 af 31. maj 2000 om behandling af personoplysninger.
[141] Institut for Menneskerettigheders høringssvar af 11. februar 2013 om ændring af lov om etablering af et udvalg om forsvarets og politiets efterretningstjenester.
[142] Institut for Menneskerettigheders høringssvar af 8. juni 2012 om betænkning nr. 1529/2012 om PET og FE samt høringssvar af 11. februar 2013 om ændring af lov om etablering af et udvalg om forsvarets og politiets efterretningstjenester.

[143] Retsplejelovens §§ 298 og 169 samt nærmere herom Emil Bock Greve: "Politiets Efterretningstjeneste. En retlig belysning af tjenestens virksomhed og det samlede kontrolsystem", Djøfs Forlag (2014), side 261ff.
[144] Ombudsmandslovens § 14 samt nærmere herom Emil Bock Greve: "Politiets Efterretningstjeneste. En retlig belysning af tjenestens virksomhed og det samlede kontrolsystem", Djøfs Forlag (2014), side 225ff.
[145] FE-lovens § 15.
[146] Kongelig Resolution af 3. oktober 2011.
[147] Institut for Menneskerettigheders høringssvar af 4. marts 2014.
[148] Forsvarsministeriets retningslinjer vedrørende behandling af data i og fra Center for Cybersikkerheds netsikkerhedstjeneste af 30. juni 2014, er tilgængelig på: http://fe-ddis.dk/cfcs/omos/Loveogregler/Pages/BehandlingafdataiogfraCenterforCybersikkerhedsnetsikkerhedstjeneste.aspx.
[149] Lov nr. 1567 af 15. december 2015 om net- og informationssikkerhed.
[150] Institut for Menneskerettigheder, Høring over forslag til lov om net- og informationssikkerhed, 7. maj 2015.
[151] Lov nr. 1571 af 15. december 2015 om ændring af lov om Forsvarets Efterretningstjeneste (Styrket indsats mod aktiviteter i udlandet, der kan indebære en terrortrussel mod Danmark og danske interesser).
[152] Institut for Menneskerettigheder, 'Høring over udkast til lov om ændring af lom om Forsvarets Efterretningstjeneste', 4. maj 2015.

INSTITUT FOR
MENNESKE
RETTIGHEDER