INSTITUT FOR MENNESKE RETTIGHEDER

DATA-BESKYTTELSE

STATUS 2013

DATABESKYTTELSE
STATUS 2013DATA-BESKYTTELSE
Dette kapitel er en del af Institut for Menneskerettigheders rapport 'Menneskerettigheder i Danmark, Status 2013'. Rapporten behandler udvalgte menneskeretlige emner og giver anbefalinger til forbedring af menneskeretsbeskyttelsen i Danmark.

Rapporten behandler emner om gennemførelse af menneskeretten, asyl, børn, databeskyttelse, frihedsberøvelse, handicap, køn, magtanvendelse, menneskehandel, race og etnisk oprindelse, religion, retfærdig rettergang, statsborgerskab, uddannelse, udvisning og udlevering, 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.STATUS 2013

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 f.eks. store typer, korte linjer, få orddelinger, løs bagkant og stærke kontraster. Vi arbejder på at få flere tilgængelige pdf'er og letlæste resumeer. Læs mere om tilgængelighed på www.menneskeret.dk.

INDHOLD

FORKORTELSER

CPR	FN's konvention om civile og politiske rettigheder
EDPS	Den Europæiske tilsynsførende for databeskyttelse
EMD	Den Europæiske Menneskerettighedsdomstols
EMRK	Den Europæiske Menneskerettighedskonventions
ENISA	European Network and Information Security Agency
EU	Den Europæiske Union
FE	Forsvarets Efterretningstjeneste
FN	De Forenede Nationer
FTC	USA's føderale handelskommission
PIA	Privatlivsimplikationsanalyse
TEUF	Traktaten om den Europæiske Unions Funktionsmåde
TI	Teleindustrien
PET	Politiets Efterretningstjeneste

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. Ofte vil ressourcestærke borgere være mindre udsatte, fordi de i mindre udstrækning interagerer med de offentlige myndigheder.

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 elektronisk databehandling 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 data-beskyttelsesperspektiv stiller et gennemregistreret og digitaliseret samfund imidlertid skærpede krav til, at de retningslinjer og procedurer, der skal beskytte borgerens rettigheder og privatliv, rent faktisk overholdes af såvel offentlige myndigheder som private virksomheder. Dette har, ikke mindst i lyset af kommunalreformen, medført en øget udveksling af oplysninger i den offentlige forvaltning.

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 stiller 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. Endvidere er der intet offentligt organ, der har de fornødne ressourcer til at dække den meget brede vifte af problemstillinger, der knytter sig til privatliv og databeskyttelse for såvel offentlige som private

virksomheder. Emnerne er ofte teknisk og samfundsmæssigt meget komplekse og rækker ud over den juridiske vurdering af, hvorvidt persondataloven overholdes. Ligeledes er der ikke nogen fast praksis for, at ny lovgivning og forvaltningspraksis skal gennemgå en privatlivsimplikationsanalyse (Privacy Impact Assessments (PIA)), det vil sige en analyse af, hvordan det pågældende forslag vil påvirke 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 til gengæld aldrig blevet underlagt en privatlivsimplikationsanalyse.

Andre væsentlige temaer, der ikke behandles her, omfatter blandt andet udveksling af oplysninger i den offentlige sektor, brug af biometriske data, overvågning i det offentlige rum, adgang til data på borgerens computer, central lagring af borgeres private nøgler (NemID) samt udveksling af oplysninger inden for EU og med USA.

I dette kapitel 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 tele- og internetudbydernes logning af kommunikationsdata, borgeres beskyttelse ved brug af sociale medier, myndigheders kontrol af sociale ydelser, lagring af personoplysninger via åbne net (cloud computing) samt lovregulering af politiets efterretningstjeneste.

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 civile og politiske rettigheder (CPR), FN's konvention om barnets rettigheder (Børnekonventionen) og FN's konvention om rettigheder for personer med handicap (Handicap-konventionen).[3]

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.[4]

Konventionen fastsætter også regler om blandt andet adgang til kendskab om elektroniske registre med mere.

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.[5] EU-retsakter vedrørende behandling af personoplysninger, og den nationale gennemførelse heraf skal respektere bestemmelserne i EU-chartret. Desuden har EU i 1995 vedtaget et databeskyttelsesdirektiv, der er grundlaget for den danske persondatalov. EU's databeskyttelsesdirektiv har siden 2010 været under revision, blandet andet for at sikre en mere opdateret og sammenhængende tilgang til databeskyttelse inden for EU.[6] Også artikel 16 i Traktaten om den Europæiske Unions Funktionsmåde (TEUF) omhandler databeskyttelse.

Aktuelt forhandles nye regler for databeskyttelse i EU (persondataforordningen). De nye regler forventes vedtaget i 2013/2014. Ligeledes forhandles et direktiv om behandling af personoplysninger på det strafferetlige område.[7]

I henhold til EU's databeskyttelsesdirektiv er der på EU-plan i øvrigt nedsat en såkaldt "artikel 29-arbejdsgruppe". Arbejdsgruppen er et rådgivende og uafhængigt EU-organ for privatliv og databeskyttelse. Gruppen består af EU-landenes respektive datatilsyn samt Den Europæiske Tilsynsførende for Data-beskyttelse. Gruppen vedtager en række henstillinger, udtalelser og notater, som forholder sig til aktuelle spørgsmål og lovgivning på databeskyttelsesområdet. Danmark tager del i dette arbejde.

Se også kapitlet 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.[8] 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".[9]

Persondataloven regulerer offentlige og privates omgang med personoplysninger og skal sikre, at Danmark lever op til EU-reglerne på området. Ved person-oplysninger 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.

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 data-ansvarlige). 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.

Datatilsynet fører tilsyn med de dataansvarliges overholdelse af persondataloven. Dette sker ved, at de 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 registrerede sager i Datatilsynet i perioden 2006-2010 er angivet i tabel 3.1.

Tabel 3.1 Antal registrerede sager i Datatilsynet, 2006-2010 fordelt efter sagstype og den procentvise udvikling i sager fra 2009-2010[10]

	2006	**2007**	**2008**	**2009**	**2010**	**Procentvis stigning i sager i 2010 i forhold til 2009**
Datatilsynets egen administration etc.	176	222	209	214	237	11%
Lovforberedende arbejde	244	245	238	329	383	16%
Forespørgsler og klager – private	646	661	861	960	1296	35%
Forespørgsler og klager – offentlige	430	360	458	508	722	42%
Sager på Datatilsynets eget initiativ	95	111	160	170	129	-24%
Sikkerhedsspørgsmål	19	14	24	30	52	73%
Internationale sager	139	133	148	157	168	7%
Kompetence iht. anden lovgivning	20	12	14	39	18	-54%
Sager i alt (ekskl. anmeldelser)	1.769	1.758	2.112	2.407	3.005	25%
Private anmeldelser	1.855	1.943	2.287	2.077	2.276	10%
Offentlige anmeldelser	744	1.729	643	375	384	2%
I alt	**4.368**	**5.430**	**5.042**	**4.859**	**5.665**	17%

I 2011 var det samlede antal sager på 5.442, det vil sige et fald på 4 procent i forhold til 2010.[11]

KAPITEL 4

4 HER KAN MENNESKERETTIGHEDERNE STYRKES I DANMARK

4.1 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 et EU-direktiv herom (lognings-direktivet).

4.1.1 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 og EU-chartret. Desuden er krav til databehandlingen fastlast 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 dette indgreb 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 lognings-direktivet, at opbevaring af telekommunikationsdata udgør et indgreb i retten til privatliv hjemlet i EMRK samt i EU-chartret.[12] 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.[13] 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".[14] En lang række organisationer har rejst en tilsvarende kritik af logningspligten.[15]

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".[16] Senest er emnet behandlet i FN's særlige rapportørs rapport om ytringsfrihed og retten til privatliv fra april 2013. Rapporten understreger, at der er et påtrængende behov for at revidere national lovgivning, der regulerer staters adgang til kommunikationsdata, og sikre, at denne er overensstemmende med de menneskeretlige standarder.[17]

4.1.2 DANSKE FORHOLD

Som led i anti-terrorpakke I vedtog Danmark i juni 2002 en logningspligt.[18] Logningspligten pålægger teleudbydere at opbevare oplysninger om borgeres kommunikation via telefon og internet i et år.[19] Oplysningerne opbevares hos teleudbyderne og stilles til rådighed for politiet i konkrete sager på grundlag af en retskendelse. Anti-terrorpakke 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 med logningsbekendtgørelsens ikrafttræden.[20] 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.[21] 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 logningspligten. I juni 2011 kom det via et notat fra Justitsministeriet frem, at man fra den daværende regerings side arbejdede på at udvide logningspligten til

blandt andet at omfatte registrering af brugere af internetcaféer, hotspots (steder, der tilbyder trådløs internetadgang) og internetadgang på biblioteker.

Logningsbekendtgørelsen gennemfører EU's logningsdirektiv fra 2006.[22] EU-direktivet blev i forbindelse med vedtagelsen udsat for kritik fra blandt andet Artikel 29-gruppen, hvorfor det blev vedtaget at tage direktivet op til revision i 2010. Forslag til revision af logningsdirektivet forventes fremsat i løbet af 2013, eller eventuelt 2014. Aktuelt bliver direktivet prøvet ved EU-domstolen foranlediget af den irske organisation Digital Rights Ireland. Ligeledes har den østrigske forfatningsdomstol sat spørgsmålstegn ved direktivets overensstemmelse med EU-chartret. I Slovakiet har en gruppe folketingsmedlemmer indbragt direktivet for den slovakiske forfatningsdomstol, ligesom forfatningsdomstole i Tyskland, Cypern, Ungarn, Tjekkoslovakiet og Rumænien har påpeget direktivets helt eller delvise uforenelighed med national lovgivning og/eller med artikel 8 i EMRK.[23] I maj 2013 afgjorde EU-domstolen, at Sverige skulle betale 3 millioner euro for forsinkelser med at implementere direktivet i svensk ret.[24]

I lighed med EU-direktivet indeholder også den danske anti-terrorlov en revisionsbestemmelse, 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.[25] Det fremgik af bemærkningerne til lovudkastet, at evalueringen var baseret på udtalelser fra Rigsadvokaten, Rigspolitiet og Politiets Efterretningstjeneste. Forslaget om at ophæve revisionsbestemmelsen blev mødt med kritik fra en række organisationer, herunder fra Institut for Menneskerettigheder, der foreslog, at der i stedet gennemførtes en bredere evaluering af logningsreglerne, hvori også indgik ordningens konsekvenser for teleudbyderne samt konsekvenserne for beskyttelsen af retten til privatliv.[26] Som led i evalueringen bør indgå alternative modeller, der kan tjene det efterforskningsmæssige formål, eksempelvis fremadrettet datafrysning på baggrund af konkret mistanke. Det fremgik af høringssvarene, at de oplysninger, der blev indhentet med hjemmel i logningsbekendtgørelsen, i overvejende grad vedrørte kriminalitet, der ikke var terrorrelateret, samt at der kun i meget begrænset omfang blev indhentet data vedrørende internettrafik.

Ligeledes har Teleindustrien (TI) flere gange fremført, at registreringen i perioden har udviklet sig dramatisk. Ved logningsbekendtgørelsens ikrafttræden i 2007 forventede myndighederne, at der årligt ville blive registreret cirka 15.000 oplysninger pr. borger. Imidlertid vurderer TI, at der i 2010 blev foretaget cirka 100.000 registreringer pr. borger svarende til cirka 550 mia. registreringer på

årsbasis.[27] Dette tal er i 2012 steget til cirka 144.000 registreringer pr. borger svarende til cirka 900 mia. registreringer på årsbasis. 90 procent af disse registreringer vedrører såkaldte sessionslogninger, det vil sige logning af, hvordan en bruger benytter internettet fra computer eller smartphone. EU-direktivet indeholder ikke noget krav om sessionslogning, og de data, som opsamles i Danmark, bliver kun i meget begrænset omfang efterspurgt eller anvendt af politiet.[28] Ifølge Justitsministeriets indberettede oplysninger til EU-Kommissionen førte logningspligtens cirka 550 mia. registreringer i 2010 til 4.235 indgreb, hvoraf de 243 tilfælde angik internetsessioner og e-mail-kommunikation.[29]

Med hensyn til omkostningerne vurderer telebranchen, at de samlet har afholdt omkostninger til at indrette systemer i en størrelsesorden på 100 mio. kr. Hertil kommer løbende driftsomkostninger, som er anslået til 50 mio. kr. årligt til data-opsamling, opbevaring og håndtering af data. På en høring i februar 2011 rejste TI blandt andet spørgsmål om omfanget af logningen i Danmark, og hvorvidt der er grundlag for at have regler, der er mere omfattende, end hvad man ser i for eksempel Sverige og Tyskland. I Sverige har man været tilbageholdende med at kræve registreringer af internettrafik, ligesom kravet om opbevaring af data kun er et halvt år.[30]

I november 2011 foreslog justitsministeren, at revisionen af de danske logningsregler skulle udsættes til 2013-2014.[31] Efter en høring i Retsudvalget, vedtog et folketingsflertal i maj 2012, at det inden udgangen af 2012 skulle undersøges, hvorvidt logningsdirektivet er en "overimplementering" af EU-reglerne. Resultatet af denne undersøgelse blev fremlagt i december 2012.[32] I forhold til sessionslogning oplyser politiets efterretningstjeneste, at det i meget begrænset omfang har været relevant at indhente sådanne oplysninger i forbindelse med efterforskning.[33] Justitsministeren fremsatte samtidig med redegørelsen forslag om at udsætte revisionen af logningsbekendtgørelsen til folketingsåret 2014-2015, hvilket mødte kritik fra Institut for Menneskerettigheder, Rådet for Digital Sikkerhed m.fl. Lovforslaget blev vedtaget den 3. juni 2013.[34]

4.1.3 ANBEFALINGER

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

- gennemfører en uafhængig evaluering og analyse af lognings-bekendtgørelsens anvendelse og effekt, særligt på de områder, hvor den danske regulering går længere end EU-direktivet (for eksempel sessionslogning og lagringsperioder). Evalueringen bør blandt andet vurdere

muligheden for at styrke de retssikkerhedsmæssige garantier, herunder at logningen sker i mindst muligt omfang og i kortest muligt tidsrum. Evalueringen bør inddrage erfaringerne fra EU-Kommissionens evaluering[35] samt erfaringer fra alle relevante parter i Danmark, herunder politi, efterretningsvæsen, advokater og forsvarere, teleindustri, de berørte udbydere samt andre relevante organisationer.

4.2 SOCIALE MEDIER

Sociale medier som for eksempel Facebook, som 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.

4.2.1 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 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 databeskyttelse efter de standarder, der er fastlagt i EU's persondatadirektiv. Private virksomheders behandling af personoplysninger er omfattet af EU's persondatadirektiv på linje med offentlige institutioner.

I juni 2009 udgav Artikel 29-gruppen en udtalelse om, hvorledes den europæiske databeskyttelse påvirker sociale medier som Facebook og Myspace.[36] 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.[37]

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 menneskerettigheder i forbindelse med brug af sociale medier.[38] Anbefalingen

understreger blandt andet, at medlemsstaterne skal sikre, at brugerne er bekendt med betingelserne for at deltage i sociale medier i en form, som er umiddelbart tilgængelig, herunder særligt 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.

4.2.2 DANSKE FORHOLD

Brugen af sociale medier som for eksempel Facebook har været markant stigende i Danmark de seneste fem 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.

Aktuelt har Facebook 800 mio. registrerede brugere, hvoraf ca. 3 mio. brugere befinder sig i Danmark og 25.000 i Grønland. Facebook fungerer ved, at brugeren opretter en profil og under denne publicerer diverse informationer, musik, billeder m.m., som enten er rettet mod brugerens "venner" eller er generelt tilgængelige, alt efter den enkeltes indstillinger. De vilkår, hvorunder brugeren offentliggør og deler information, er svære at gennemskue, og Facebook bliver i stigende grad kritiseret for at indsamle og videregive store mængder af oplysninger om tjenestens brugere – for eksempel til de tredjeparts-programmer (apps), som de samarbejder med. 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.[39] 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.

De nordiske datatilsyn kontaktede i juli 2011 Facebook for at få større klarhed over virksomhedens behandling af personoplysninger.[40] 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 virksomheder, de 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 andre virksomheder, som Facebook samarbejder med.[41]

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 det tyske datatilsyn 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, men at der ikke kan stilles krav til Facebook efter tysk persondatalov, idet Facebook ikke behandler personoplysninger i Tyskland. Det tyske tilsyn har udtrykt forundring over afgørelsen, da Facebook heller ikke behandler persondata i Irland (dette sker alene i USA).[42]

I oktober 2011 anlagde en jurastuderende i 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 hos Facebook i Irland i efteråret 2011, og som resulterede i en rapport og en række anbefalinger til Facebook. Facebook har efterfølgende givet tilsagn om at følge en række 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.[43] En opfølgende inspektion blev gennemført i juli 2012.

I november 2011 indgik USA's føderale handelskommission (FTC) et forlig med Facebook, 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.[44]

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".[45] Dette skyldes ifølge Datatilsynet, at Facebook er hjemhørende i Irland og således er 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 givent 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 tre mio. danske brugere. Derudover virker det ikke realistisk, at det irske datatilsyn skal varetage persondatabeskyttelsen på vegne af samtlige EU-borgere.

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 Facebook kan fastsætte rammerne for aftalen gennem et sæt standardvilkår. Af disse 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.[46] Ombudsmanden har udtalt, at oplysninger på Facebook kan være offentligt tilgængelige på mange måder afhængig af for eksempel ens privatlivsindstillinger og antallet af ens Facebook-venner. Man må altså foretage en konkret afvejning, blandt andet ud fra, hvor let tilgængelige 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.

Der henvises i øvrigt til statusrapportens kapitel om ytringsfrihed.

4.2.3 ANBEFALINGER

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

- foretager en udredning af de konsekvenser, som brugen af sociale medier måtte have for ytrings- og informationsfriheden samt retten til respekt for privatlivet

- udarbejder materiale, som på en let tilgængelig måde redegør for brugerens rettigheder og vilkår ved brug af sociale medier som Facebook. Materialet bør blandt andet tage sigte mod lærere og elever i folkeskolen

- undersøger, hvordan det danske tilsyn med sociale mediers opbevaring og udveksling af personoplysninger kan skærpes og kortlægger, hvordan andre EU-lande håndhæver national lovgivning over for sociale medier.

4.3 KONTROL MED OFFENTLIGE YDELSER

I Danmark har myndighederne efter nærmere regler adgang til på forskellige måder at kontrollere borgernes private forhold med henblik på at bekæmpe socialt bedrageri.

4.3.1 DEN MENNESKERETLIGE BESKYTTELSE

Kontrol af borgeres personlige forhold udgør indgreb i de pågældende personers privatliv, som er beskyttet i blandt andet EMRK artikel 8. For at et indgreb i privatlivet er lovligt, er det blandt andet en forudsætning, at indgrebet har lovhjemmel. Dette krav indebærer efter Den Europæiske Menneskerettighedsdomstols (EMD) praksis blandt andet, at den nationale lovgivning skal opfylde visse kvalitative krav, herunder at retstilstanden skal være forudsigelig, og at reglerne skal være tilstrækkeligt klare og præcise. Det skal være muligt for de berørte at overskue og forudsige konsekvenserne af reglernes anvendelse og dermed beskytte sig mod hjemlede indgreb. Ud over kravet om lovhjemmel er det endvidere en forudsætning, at indgrebet er begrundet i et anerkendt hensyn samt nødvendigt, herunder proportionalt.

4.3.2 DANSKE FORHOLD

Der har det seneste år været en del debat om myndighedernes mulighed for at kontrollere borgernes private forhold med henblik på at bekæmpe socialt bedrageri. Et eksempel herpå har været de kommunale kontrolgruppers praksis. Kontrolgrupperne blev oprettet fra 1999 og frem som led i kommunernes opgave med at administrere de sociale ydelser, herunder sikre, at ydelserne udbetales på det grundlag og efter de kriterier, som er fastlagt i lovgivningen på det pågældende område.[47]

Spørgsmålet om kontrolgruppernes praksis, herunder deres mulighed for at overvåge borgeres fysiske og virtuelle adresser og anvende eventuelt ulovligt indsamlet materiale, blev i april 2011 behandlet i Folketingets Retsudvalg. Her

fastslog beskæftigelsesministeren, at overvågning som udgangspunkt må betragtes som en politimæssig opgave. Er der begrundet mistanke om, at der er tale om socialt bedrageri, bør kommunen derfor melde borgeren til politiet, som derefter foretager den videre efterforskning i overensstemmelse med retsplejelovens regler. Samtidig angav ministeren, at en kommune ikke er helt udelukket fra at kunne observere en borger, der modtager sociale ydelser. Kommunen skal ved eventuel overvågning overholde proportionalitetsprincippet, det vil sige vælge det mindst indgribende middel. Ministeren henviser blandt andet til Beskæftigelsesministeriets vejledning til lov om børnetilskud, hvori det fremgår, at overvågning af borgere, der modtager børnetilskud, ofte vil være en uproportional fremgangsmåde. Det skyldes, at overvågninger en meget vidtgående måde at skaffe sig oplysninger om borgere på.

I en udtalelse fra marts 2013 understreger ombudsmanden, at afgørelser om standsning af udbetaling af sociale ydelser og tilbagebetaling ofte er ganske indgribende for den enkelte borger og kan være velfærdstruende. I den konkrete sag konkluderede ombudsmanden, at kommunen ikke havde været opmærksom på reglerne i tvangsindgrebsloven, herunder vejledt den pågældende tilstrækkeligt i forbindelse med sagen. Ombudsmanden var tillige kritisk over for de oplysninger, som myndighederne havde lagt vægt på – herunder den centrale brug af en anonym anmeldelse.[48]

Specifikt i forhold til brug af oplysninger fra Facebook udtalte ombudsmanden i januar 2011, at der, hvis en person har en åben profil på Facebook, i realiteten er tale om, at oplysningerne er offentligt tilgængelige. Det samme kan være tilfældet, hvis en person har et stort antal venner på Facebook. Personoplysninger, der er offentligt tilgængelige, kan som udgangspunkt frit behandles af myndighederne, dog skal behandlingen være saglig, og oplysningerne relevante for sagen.[49]

Et andet eksempel vedrører de regler om lufthavnskontrol, der blev indført i 2011 som led i en skærpet kontrol med misbrug af offentlige ydelser.[50] Ændringerne indebar, at Pensionsstyrelsen nu har adgang til at udføre kontrolaktioner i lufthavne og andre afgrænsede offentlige steder. Pensionsstyrelsen kan således afkræve oplysninger af en bred gruppe af borgere i lufthavne, på banegårde osv. med henblik på at sikre, at de borgere, der skal opholde sig i Danmark som forudsætning for at modtage en offentlig ydelse, rent faktisk opholder sig i landet. Pensionsstyrelsen kan i den forbindelse uden videre foretage kontrol af de rejsendes personlige papirer i form af pas eller lignende samt slå op i e-indkomstregistret (hvoraf der kan udledes oplysninger om personens sociale forhold), uden at der er konkret mistanke rettet mod den

enkelte. Der er ikke fastsat særlige kriterier/mistankekrav for udvælgelse af personer til kontrol, og der er således tale om en helt generel adgang til kontrol, der kan indebære kontrol af et stort antal uskyldige rejsende. Det er i øvrigt uklart, hvorledes den enkelte borger kan klage over Pensionsstyrelsens kontrol af den pågældende, og hvorvidt der føres tilsyn med Pensionsstyrelsen i den forbindelse.[51] Ankestyrelsen har i en principafgørelse fastlagt, at hvis den faktiske forvaltningsvirksomhed er af særligt indgribende karakter, så kan denne ankes, selvom dette som udgangspunkt ikke er en mulighed.[52]

Ved årsskiftet 2012/2013 overtog myndigheden Udbetaling Danmark en række udbetalingsopgaver fra kommunerne på områderne folke- og førtidspension, boligstøtte, barselsdagpenge og familieydelse. Dette ændrer ikke ved kommunernes praksis for kontrolaktioner, men indebærer en ny samarbejdsmodel mellem kommunerne og Udbetaling Danmark således, "at der i tæt samarbejde tilvejebringes oplysninger om, hvorvidt der snydes med sociale ydelser. Den nye samarbejdsmodel tager hensyn til, at kommunerne fortsat skal kunne foretage kontrol af sociale sager, og at kommunerne fortsat kan udnytte kendskab til lokalområdet eller nærheden til borgeren, når en sag skal oplyses".[53] Udbetaling Danmark har i den nye model den endelige afgørelseskompetence, blandt andet med det formål at sikre en mere ensartet praksis for, hvordan sager oplyses i hele landet.[54] Lov om Udbetaling Danmark (§§ 9-11) giver kommunerne og Udbetaling Danmark en bred hjemmel til at udveksle oplysninger, der er nødvendige i forbindelse med kontrol af sociale ydelser uden samtykke fra borgeren.[55]

4.3.3 ANBEFALINGER

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

- fastsætter objektive og saglige kriterier for udvælgelsen af personer til kontrol for misbrug af sociale ydelser, så udvælgelsen er afgrænset og baseret på konkrete data

- fastsætter udtrykkelige regler om klageadgang og tilsyn i forbindelse med kontroller samt sikrer adgang til genopretning, hvis borgerens sociale ydelser uberettiget har været standset

- overvåger anvendelsen af kontrolaktioner, herunder beskriver omfanget af kontrolaktioner og resultaterne heraf, så antallet af resultatløse og dermed konkret ubegrundede kontrolaktioner kan opgøres

- sikrer, at der ved mistanke om strafbart forhold sker anmeldelse af forholdet til politiet, og sikrer, at lovkrav til tvangsindgreb overholdes.

4.4 CLOUD COMPUTING

Cloud computing 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.

4.4.1 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.

Det er aktuelt uafklaret, hvilke data der må placeres i en cloud computing-tjeneste, samt hvorvidt de skærpede beskyttelseskrav, som stilles i forbindelse med følsomme personoplysninger, kan opfyldes i en cloud computing-tjeneste. Dertil kommer spørgsmål forbundet med at lade personoplysninger transmittere over åbne net og opbevare dem i et andet land, herunder udfordringen med at håndhæve EU’s databeskyttelsesdirektiv over for tredjelande. I udgangspunktet må der kun overføres oplysninger til et tredjeland, såfremt dette land sikrer et tilstrækkeligt beskyttelsesniveau.

I en udtalelse fra juli 2012 analyserer Artikel 29-gruppen brug af cloud computing i lyset af EU's persondatabeskyttelse.[56] Gruppen konkluderer blandt andet, at virksomheder og offentlige instanser, der ønsker at bruge cloud-tjenester, bør gennemføre en omfattende risikovurdering forud for indførelsen af sådanne tjenester. Det anbefales 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.

4.4.2 DANSKE FORHOLD

Cloud computing indebærer en ”internetbaseret adgang til en delt pulje af konfigurerbare it-ressourcer (net, servere, datalager, programmer og services)”.[57]

Cloud computing er en relativt ny model for dataopbevaring. Emnet blev i 2010 behandlet af regeringens it-sikkerhedskomité, der udgav rapporten ”Sikkerhed i Cloud Computing”.[58] 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.[59] I april 2011 foranlediget af en sikkerhedsbrist i forbindelse med Kommunernes Landsforenings overførsel af et køreprøve-bookingsystem til en cloud-løsning.[60] Og i 2012 på baggrund af en henvendelse fra Microsoft vedrørende brug af cloud-tjeneste i Office 365-pakken.[61] Ligeledes har det svenske datatilsyn i juni 2013 forholdt sig til offentlige myndigheders brug af Google Apps.[62]

I sagen vedrørende Odense kommune angav Datatilsynet blandt andet, at en eventuel overførsel af oplysninger til datacentre, som er beliggende i andre usikre tredjelande end USA, 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.[63] 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 anbefaler, at myndigheder benytter den tjekliste, som European Network and Information Security Agency (ENISA) har udarbejdet, i forhold til at risikovurdere cloud-tjenester.[64]

I den konkrete sag udtalte Datatilsynet endvidere, at overførsel af oplysninger til datacentre, som befinder sig i EU-medlemsstater eller EØS-lande, ikke udgør tredjelandsoverførsler omfattet af persondataloven. Derimod vil overførsel af oplysninger til datacentre i USA og visse lande i Europa udgøre en tredjelands-overførsel omfattet af persondataloven. 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.
Sagen rejser en række generelle og uafklarede 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.

Teknologirådet har tidligere anbefalet, at der gennemføres en privatlivs-implikationsanalyse (PIA) forud for indførelse af it-systemer i den offentlige forvaltning.[65] En sådan analyse skal vurdere, hvilke konsekvenser systemerne har for de praktiske muligheder for at leve op til "god databehandlingsskik" og persondatalovens øvrige regler. Ligeledes har den daværende IT- og Telestyrelse, i samarbejde med Dansk Industri (ITEK), i 2007 lavet en skabelon for gennemførelse af privatlivsimplikationsanalyse, primært rettet mod it-kunder og leverandører.[66] Senest har Digitaliseringsstyrelsen i maj 2013 udsendt en Guide til konsekvensvurdering af privatlivsbeskyttelse.[67] Guiden har ikke været sendt i høring. Der er i dag ikke krav til offentlige myndigheder om at udarbejde en analyse af de privatlivsmæssige implikationer forud for indførelse af nye it-løsninger eller it-strategier, der behandler personoplysninger.

4.4.3 ANBEFALINGER

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

- sikrer, at der udarbejdes en analyse af de privatlivsmæssige implikationer forud for indførelse af it-løsninger, der behandler personoplysninger, herunder cloud computing

- styrker den uafhængige analyse og rådgivning i relation til privatliv og databeskyttelse i forbindelse med de mange offentlige digitaliserings-projekter, der gennemføres i disse år.

4.5 LOVREGULERING AF POLITIETS EFTERRETNINGSTJENESTE

Politiets Efterretningstjeneste (PET) er sammen med Forsvarets Efterretningstjeneste (FE) Danmarks sikkerhedstjeneste og udgør en del af det danske politi, hvis virksomhed er reguleret i politiloven.[68] 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, beslaglæggelse mv.

PET's virksomhed har hidtil ikke været reguleret ved lov, men alene været fastlagt i instrukser, retningslinjer mv., ligesom PET heller ikke er omfattet af persondataloven. Der er i sommeren 2013 vedtaget en lov for PET's virksomhed, som træder i kraft den 1. januar 2014.[69] Lovteksten 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. Samtidigt med at lovforslaget vedrørende PET blev fremsat, blev der tillige fremsat lovforslag vedrørende en styrkelse af Folketingets Kontroludvalg[70] og lovforslag vedrørende en lovregulering af FE.[71] Begge lovforslag er efterfølgende vedtaget med ikrafttræden den 1. januar 2014.[72] I dette tema fokuseres på nogle af de menneskeretlige problemstillinger, som reguleringen af PET rejser i forhold til beskyttelse af retten til privatliv og demokratisk kontrol.

4.5.1 DEN MENNESKERETLIGE BESKYTTELSE

Offentlige myndigheders, herunder politiets og efterretningstjenesters, indsamling, registrering, behandling og opbevaring af personoplysninger mv. skal iagttage EMRK artikel 8, Europarådets konvention om beskyttelse af det enkelte menneske i forbindelse med elektronisk databehandling af personoplysninger, 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.[73] 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.[74] 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 persondataloven, hvis det er nødvendigt).[75] 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. EU behandler for tiden et direktiv om behandlingen af personoplysninger på det strafferetlige område[76] og en forordning om et nyt retsgrundlag for Europol.[77] Sidstnævnte fastsætter høje standarder for databeskyttelse.

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 35 anbefalinger for "god praksis" i forbindelse med den retlige og institutionelle ramme for efterretningstjenester og tilsynet med disse.[78]

4.5.2 DANSKE FORHOLD

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 vedrører en ny lov for PET, herunder oprettelse af et nyt tilsyn med efterretningstjenesterne (PET-tilsynet) til afløsning af Wamberg-udvalget og en styrkelse af Folketingets Kontroludvalg. Den nye lov for PET svarer i det væsentlige til det lovudkast, der blev udsendt til høring i 2012, og hvor Institut for Menneskerettigheder m.fl. afgav høringssvar.[79] Se nærmere herom og om PET på Institut for Menneskerettigheders hjemmeside.[80] Loven er vedtaget den 30. maj 2013 og træder i kraft den 1. januar 2014. Reguleringen skal ses i sammenhæng med en ændring af loven vedrørende Folketingets Kontroludvalg til styrkelse af udvalget.[81]

Institut for Menneskerettigheder har i høringsfasen blandt andet påpeget, at forslaget til ny PET-lov primært fokuserer på PET's behandling af personoplysninger og mangler et tilsvarende fokus på andre områder af PET's virksomhed. Det samme gælder PET-tilsynets virksomhed efter loven, idet tilsynet primært skal føre tilsyn med PET's behandling af personoplysninger og ikke PET's arbejde i marken, herunder for eksempel brugen af agenter.

Den nye lov for PET ændrer ikke ved PET's arbejdsopgaver, men fastsætter nye regler for PET's adgang til at indsamle, bearbejde, registrere og videregive personoplysninger mv. De betingelser, der opstilles for PET's behandling af oplysninger, er baseret på persondatalovens standarder.[82] Loven svarer – som ovenfor nævnt – i hovedtræk til PET-udvalgets lovudkast.

Der er imidlertid afvigelser på blandt andet følgende områder: Lovens regler for behandling af personoplysninger gælder modsat det oprindelige forslag for PET's behandling af oplysninger om "enhver person", uanset om denne er hjemmehørende i Danmark. 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 for PET's adgang til at behandle personoplysninger 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 – i overensstemmelse med regeringserklæringen fra 1968 – et forbud mod registrering alene på grundlag af lovlig politisk virksomhed, men dette forbud gælder ikke undtagelsesfrit. PET vil – som det er tilfældet i dag – 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 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 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).

Det nyoprettede PET-tilsyn skal efter loven bestå af fem medlemmer, der udpeges af justitsministeren efter drøftelse med Kontroludvalget (med undtagelse af formanden, som udpeges af landsretternes præsidenter). Mens Wamberg-udvalgets kontrol primært sker i form af forudgående godkendelser, for eksempel af registrering af personoplysninger, skal det nye PET-tilsyn derimod ved en efterfølgende kontrol kunne prøve PET's registreringer stikprøvevist eller i konkrete sager, hvor tilsynet i lighed med Ombudsmanden går ind i af egen drift eller efter klage fra en borger. Tilsynet inddrages dermed ikke i PET's beslutningsproces. Tilsynet udstyres ikke med kompetence til at kunne påbyde PET bestemte foranstaltninger i forhold til behandlingen af oplysninger.

Efter loven har en person ikke ret til indsigt i oplysninger, som PET behandler om personen. Der er heller ikke ret til at få oplyst, om PET overhovedet behandler oplysninger om personen. Derimod etableres der efter loven en adgang for personen til at kunne anmode PET-tilsynet om at undersøge, om PET på et uberettiget grundlag behandler oplysninger om borgeren. Fysiske personer og juridiske personer, der Ikke er hjemmehørende i Danmark, bliver tillige omfattet af indsigtsretten.

Styrkelsen af Folketingets Kontroludvalg indebærer, at regeringen forpligtes til at give Kontroludvalget en årlig orientering om PET's virksomhed, herunder brugen af civile agenter. Udvalget skal også orienteres 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, mens udvalget ikke udstyres med en selvstændig kontrolfunktion.[83] Udvalget vil også fremover være afhængigt af de informationer, som det modtager fra PET.

Som nævnt ovenfor har Institut for Menneskerettigheder blandt andet 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 samt kontrollen med dette. Som eksempel kan nævnes PET's brug af kontakter, meddelere og agenter.

Reguleringen og kontrollen med PET vil således være begrænset til bestemte områder for PET's virksomhed, og vil efter Institut for Menneskerettigheders opfattelse ikke leve op til internationale anbefalinger for en uafhængig og effektiv kontrol med efterretningstjenesterne i et moderne retssamfund.[84]

Instituttet afgav i forbindelse med høringen et supplerende høringssvar om PET's samarbejde med Folketingets Indfødsretsudvalg.[85]

4.5.3 ANBEFALINGER

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

- foretager en vurdering af det danske terrorberedskabs indvirkning på menneskerettigheder, herunder retssikkerhed i Danmark
- foretager en kortlægning og systematisk vurdering af det samlede tilsyn med PET
- etablerer uafhængige og effektive tilsyn og kontroller med PET's virksomhed

- genovervejer at tillægge PET-tilsynet kompetence til at kunne påbyde PET bestemte foranstaltninger i forhold til behandlingen af oplysninger

- overvejer, om adgangen til indsigt for den enkelte fysiske eller juridiske person kan udvides.

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] Jf. FN's Verdenserklæring om Menneskerettighederne artikel 12.
[3] Jf. CPR artikel 17, Børnekonventionens artikel 16, og Handicapkonventionens artikel 22.
[4] Jf. Europarådets konvention om beskyttelse af det enkelte menneske i forbindelse med elektronisk databehandling af personoplysningers artikel 5.
[5] Jf. EU-charterets artikel 8.
[6] 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.
[7] 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. Tilgængelig på: www.eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0010:FIN:EN:PDF.
[8] Jf. grundlovens §§ 71 og 72.
[9] Jf. grundlovens § 72.
[10] Datatilsynets Årsrapport 2010, side 4.
[11] Jf. Datatilsynets årsberetning for 2011, side 17.
[12] Jf. 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.
[13] 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.
[14] Peter Hustinx, EDPS, "The moment of truth for the Data Retention Directive", speech, Bruxelles, 3. december 2010.
[15] Jf. brev af 22. juni 2010 fra en række organisationer til Kommissær Malmström, Reding and Kroes. Tilgængelig på: www.vorratsdatenspeicherung.de/images/DRletter_Malmstroem.pdf.
[16] Jf. Article 29 Working Party: Opinion 3/2006.
[17] Se 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.

[18] 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 af 6. juni 2002.
[19] Jf. retsplejeloven § 786, stk. 4.
[20] Logningsbekendtgørelsen af 28. september 2006.
[21] Jf. oversigt over høringssvar, Justitsministeriet, 14. december 2011. Tilgængelig på: http://webarkiv.ft.dk/img20012/udvbilag/lib9/20012_1119.pdf.
[22] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC.
[23] For en oversigt over status i respektive EU-lande jf. EU-Kommissionens evalueringsrapport fra 18. april 2011; COM(2011) 225 final.
[24] EU-domstolen, Kommissionen mod Sverige, afgørelse af 30. maj 2013, C‑270/11.
[25] Jf. 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.
[26] Jf. Institut for Menneskerettigheders høringssvar af 16. marts 2010 om ophævelse af revisionsbestemmelsen.
[27] Jf. Telekommunikationsindustriens høringssvar af 25. november 2011 om ændring af revisionsbestemmelsen.
[28] Tallene for 2012 samt den procentvise andel, der hidrører fra sessionslogning er oplyst af Jacob Willer, formand for Teleindustrien, på Databeskyttelsesdagen på Christiansborg den 28. januar 2013.
[29] Jf. Justitsministeriets indberetning af statistiske oplysninger om logning efter EU's logningsdirektiv, 8. december 2011. Gengivet i Retsudvalget 2011-12, bilag 146.
[30] Jf. høring i Retsudvalget den 24. februar 2011. Tilgængelig på: www.ft.dk/webtv/video/20101/reu/H3.aspx?from=24-02-2011&to=24-02-2011&selectedMeetingType=&committee=&as=1#player.
[31] Jf. Forslag til lov om ændring af straffeloven, retsplejeloven mv. (Ændring af revisionsbestemmelse), 1. november 2011.
[32] Jf. Redegørelse om diverse spørgsmål vedrørende logningsreglerne, 21. december 2012, Gengivet i Retsudvalget 2012-13, Bilag 125. Tilgængelig på: www.ft.dk/samling/20121/almdel/reu/bilag/125/1200765.pdf.
[33] Redegørelse om diverse spørgsmål vedrørende logningsreglerne, 21. december 2012, Gengivet i Retsudvalget 2012-13, bilag 125, side 36.
[34] Lov nr. 635 af 12. juni 2013 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 (Ændring af revisionsbestemmelse).
[35] Jf. Report from the commission to the Council and the European Parliament, "Evaluation report on the Data Retention Directive (Directive 2006/24/EC)", COM(2011) 225 final, 18. april 2011.

Tilgængelig på: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0225:FIN:en:PDF.

[36] Jf. Article 29 Working Party: Opinion 5/2009.

[37] Jf. EC justice, Reform of data protection legislation, 6. februar 2011. Tilgængelig på: http://ec.europa.eu/justice/data-protection/index_en.htm.

[38] 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.

[39] 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.

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

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

[42] Jf. pressemeddelse fra Datatilsynet i Slesvig-Holsten den 15. februar 2013. Tilgængelig på: www.datenschutzzentrum.de/presse/20130215-verwaltungsgericht-facebook.htm.

[43] 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.

[44] 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.

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

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

[47] Jf. Vejledning fra Kommunernes Landsforening, "Fremgangsmåden i sager om misbrug af sociale ydelser", 2008, samt "Kontrol med udbetaling af sociale ydelser", revideret i 2008.

[48] Jf. Folketingets Ombudsmand: Tilbagebetaling af sociale ydelser, sagsnummer 2013-4, 12. marts 2013.

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

[50] Jf. L 187 vedtaget 1. juni 2011 (lov om ændring af lov om aktiv socialpolitik, lov om arbejdsløshedsforsikring m.v., integrationsloven og forskellige andre love).

[51] Jf. Institut for Menneskerettigheders høringssvar af 18. april 2011 om forslag til lov om ændring af lov om aktiv socialpolitik, lov om arbejdsløshedsforsikring, integrationsloven og forskellige andre love (Skærpet kontrol med udbetaling af offentlige forsørgelsesydelser m.v.)

[52] Se Ankestyrelsens principafgørelse 93-13, 20. juni 2013.

53 Jf. Aftale om kommunernes økonomi for 2012 mellem regeringen og KL, side 17.

[54] Jf. Socialudvalget, "Udbetaling Danmark og Socialt bedrageri", Socialudvalget 2011-12 L 86 Bilag 8, L 87 Bilag 8, side 4.

[55] Jf. Lov om Udbetaling Danmark af 11. april 2012.

[56] Article 29 Working Party: Opinion 05/2012.
[57] Article 29 Working Party: Opinion 05/2012, side 5.
[58] It-sikkerhedskomitéen, "Sikkerhed i Cloud Computing," december 2010.
[59] Datatilsynet, "Behandling af følsomme personoplysninger i cloud-løsning", 3. februar 2011.
[60] 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.
[61] Datatilsynet, "Behandling af personoplysninger i cloud-løsningen Office 365", 6.juni 2012.
[62] Datainspektionen, afgørelse af 31. maj 2013, sagsnummer 1351-2012. Tilgængelig på: www.datainspektionen.se/Documents/beslut/2013-05-31-salems-kommun.pdf.
[63] Jf. bekendtgørelse om sikkerhedsforanstaltninger til beskyttelse af personoplysninger, som behandles for den offentlige forvaltning af 15. juni 2000.
[64] 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.
[65] Teknologirådet, "Retssikkerhed og aktivt medborgerskab i digital forvaltning", 2005/13.
[66] Dansk Industri/ITEK, "God Privacy Praksis – en guideline for IT-leverandør og kunder", 2007.
[67] Digitaliseringsstyrelsen, "Guide til konsekvensvurdering af privatlivsbeskyttelse", maj 2013.
[68] Se lov nr. 444 af 9. juni 2004 om politiets virksomhed.
[69] Se lov nr. 604 af 12. juni 2013 om politiets efterretningstjeneste (PET).
[70] Forslag til lov om ændring af lov om etablering af et udvalg om forsvarets og politiets efterretningstjenester, L 162 2012-13, fremsat 27. februar 2013.
[71] Forslag til lov om Forsvarets Efterretningstjeneste (FE), L 163 2012-13, fremsat 27. februar 2013.
[72] Se henholdsvis lov nr. 632 af 12. juni 2013 og lov nr. 602 af 12. juni 2013.
[73]. Se Recommandation of The Committee of Ministers to member states "Regulating the use of personal data in the police sector", recommandation no. R (87) 15.
[74] Jf. Rådets rammeafgørelse af 27. november 2008 om beskyttelse af personoplysninger i forbindelse med politisamarbejde og retligt samarbejde i kriminalsager, 2008/977/RIA.
[75] Se bekendtgørelse nr. 1287 af 25. november 2010.
[76] 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.
[77] Se Institut for Menneskerettigheders høringssvar af 11. juli 2013.
[78] Jf. 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.
[79] Oversigt over høringssvar vedrørende betænkning om PET. Tilgængelig på: http://menneskeret.dk/files/images/PET%20billeder/PET%20doks/Høringssvar%20vedr%20%20PET-betænkning.pdf.

[80] Tilgængelig på: http://menneskeret.dk/news/pet.
[81] Lov nr. 632 af 12. juni 2013 om styrkelse af kontroludvalgets beføjelser.
[82] Se lov nr. 429 af 31. maj 2000 om behandling af personoplysninger.
[83] Se Institut for Menneskerettigheders høringssvar af 11. februar 2013 om ændring af lov om etablering af et udvalg om forsvarets og politiets efterretningstjenester.
[84] Se 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.
85 Se Institut for Menneskerettigheders høringssvar af 11. juni 2012 om PET's samarbejde med Folketingets Indfødsretsudvalg, afgivet i anledning af høring over betænkning nr. 1529/2012 om PET og FE.

INSTITUT FOR
MENNESKE
RETTIGHEDER