FOLKETINGET

Retsudvalget

Til: Udvalgets medlemmer
Dato: 4. september 2014

Høringssvar

Bemærkninger til Beretning nr. 3
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

Med venlig hilsen

Birgitte Toft-Petersen
Bachelorfuldmægtig

Bemærkninger til Beretning #3

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

Bemærkningerne er udarbejdet af CSC Danmark A/S.

Generelt:

Offentlige myndigheder har i en årrække fokuseret på digitalisering af det danske samfund med effektivisering og større tilgængelighed for borgere og virksomheder til følge.

I en tid hvor global cyber kriminalitet vokser med flere hundrede procent hvert år, øges kravene til at sikre personfølsomme data mod uautoriseret adgang. Den øgede digitalisering og det forværrede trusselsbillede har skabt en større bevidsthed hos offentlige myndigheder og politikere om nødvendigheden af at investere i øget sikkerhed. På denne baggrund hilser CSC nedsættelsen af en parlamentarisk arbejdsgruppe velkommen.

Bemærkninger til afsnit 2. "Politiske bemærkninger"

Styrkelse af Datatilsynet:

En styrkelse af Datatilsynet vil ikke i sig selv gøre de offentlige systemer mere sikre.

Der mangler snarere overordnede anvisninger og anbefalinger på det IT-sikkerhedsmæssige område. Anvisninger og anbefalinger, der instruerer offentlige myndigheder i, **hvordan** deres IT systemer skal sikres og overvåges, herunder også hvilke krav der stilles til nye driftsformer såsom cloud.

En evt. styrket offentlig tilsynsvirksomhed bør derfor have stærke IT-sikkerhedsmæssige kompetencer og fokusere på, at fællesoffentlige anbefalinger og anvisninger overholdes.

Logningsreglerne og personoplysningsloven:

Med den store mængde transaktioner og det deraf følgende store antal logs bør logningsreglerne opdateres til det nuværende trusselsscenarie. Der bør bl.a. stilles krav om realtids, automatiseret log-gennemgang, herunder korrelering og gennemgang af sikkerhedslogs på tværs af en bred vifte af systemer, applikationer og sikkerhedsopsætninger (FW, IDS/IPS, FIA etc.).

EU's nye databeskyttelsesforordning:

Den nye forordning vil stille krav om yderligere beskyttelse af persondata. Det er ikke på nuværende tidspunkt klart, om forordningen vil tilbyde tilstrækkelig beskyttelse af de meget store mængder af personfølsomme data, som den offentlige sektor er i besiddelse af.

Det nævnes, at Tyskland og Frankrig har været meget aktive i arbejdet med EU-forordningen, og det er også relevant at nævne andre landes meget regulerede tilgang til persondatabeskyttelse. Bl.a. har Tyskland og England udstukket retningslinjer for hvilke sikkerhedsløsninger, der skal være installeret, og hvorledes monitorering og opfølgning skal foretages. Kravene til disse sikkerhedsløsninger afhænger af, hvilke typer data der er tale om, og i hvilket omfang de betragtes som vitale i forhold til at beskytte den enkelte borger eller nationens sikkerhed.

I Danmark eksisterer der ikke lovgivning eller forordninger, der giver anvisninger på**, hvordan** forskellige typer af data skal beskyttes. Det eksisterende regelsæt er således ikke tilstrækkelig specifikt, når det gælder kategorisering af forskellige former for data. Og der mangler konkrete retningslinjer eller lovgivning, som regulerer metoder og processer til at understøtte sikkerheden. Det er i det store og hele op til de enkelte dataejere at etablere tilstrækkelig sikkerhed, uanset om dataejeren har den fornødne kompetence på sikkerhedsområdet. Konsekvensen er, at der i Danmark ikke er en koordineret og ensartet IT sikkerhed på tværs af ministerier, styrelser og andre offentlige myndigheder.

Behovet for samling af it- og datasikkerhed ved en ansvarlig ressortminister:

Der er behov for, at ansvaret for nationens IT sikkerhed samles ét sted. Ansvaret bør dække hele den offentlige sektor på tværs af alle niveauer og udstrækkes til de private virksomheder, der benytter personfølsomme data, som hentes hos det offentlige eller som administrerer samfundskritisk infrastruktur eller udfører samfundskritiske funktioner.

Det vil således være hensigtsmæssigt fremadrettet at have en mere holistisk tilgang til IT-sikkerhed, der dækker alle samfundskritiske og følsomme data og funktioner, uanset om de varetages af offentlige eller private virksomheder.

Man bør i tilknytning til etablering af én central IT-sikkerhedsmyndighed etablere et bredt samarbejde med alle IT-leverandører efter udenlandsk forbillede. Dette samarbejde skal sikre en hurtig udveksling af informationer leverandører og myndigheder imellem i tilfælde af IT-sikkerhedsmæssige hændelser.

Yderligere krav til både offentlige og private dataansvarlige:

Der bør stilles entydige, ensartede krav om sikkerhedsarkitektur og sikkerhedsrapportering til alle dataejere og deres leverandører. Hvis disse krav skal matche ”Best Practice”, vil det resultere i en ikke ubetydelig investering i yderligere sikkerhedsudstyr og løbende opfølgning.

Den offentlige sektors håndtering af IT er karakteriseret af mange mindre IT-organisationer og et noget fragmenteret dataejerskab. Det vil formodentlig ikke være økonomisk rentabelt at lade hver enkelt dataejer anskaffe og drive de nødvendige sikkerhedsløsninger. Ud over at centralisere det overordnede ansvar for sikkerhed, bør udførelsen således også samordnes.

I samarbejde med den private sektor og sikkerhedsleverandørerne bør det offentlige centralisere sikkerhedsovervågningen i større centre, der opererer 24X7, og som har det fornødne teknologiske

beredskab, hvis der måtte opstå problemer. Det er ligeledes vigtigt, at disse overvågningscentre er sammenkoblet med globale centre, der har adgang til internationale informationer om sikkerhedstrusler. Dette er vitalt for at kunne dæmme op for den omsiggribende internationale Cyber kriminalitet.

Obligatorisk databeskyttelsesvurdering af alle offentlige digitaliseringsprojekter:

Der bør fra centralt hold stilles konkrete sikkerhedskrav til alle offentlige IT-projekter. I den forbindelse vil det være en god ide at anvende erfaringer fra andre lande, som har arbejdet mere målrettet med IT sikkerhed end Danmark og derfor har haft mulighed for at påvirke IT sikkerhedsleverandørerne og deres service udbud.

En side gevinst ved dette er de lavere omkostninger, der følger af at anvende standard løsninger frem for specielt fremstillede løsninger til det relativt lille danske marked.

27.08.2014/MM
J.nr. 10-0300

DANMARKS MEDIE- OG JOURNALISTHØJSKOLE
DANISH SCHOOL OF MEDIA AND JOURNALISM

Kulturudvalget
Christiansborg
DK-1240 København K
Att.: Birgitte Toft-Petersen

ADR Olof Palmes Allé 11,
DK-8200 Aarhus N
TLF +45 89 440 440
FAX +45 86 168 910
WEB www.dmjx.dk
CVR 31111048
VAT DK-3111 1048
EAN 5798000555174
IBAN DK2902164069145620
SWIFT DABADKKK
BANK DANSKE BANK
Reg.nr. 0216, kontonr. 4069145620

Høringssvar fra Danmarks Medie- og Journalisthøjskole til beretning afgivet af Folketingets Kulturudvalg og Retsudvalg 3. juni 2014

Danmarks Medie- og Journalisthøjskole finder det positivt og vigtigt, at høringen indeholder bemærkninger om, at *demokratiet bygger på en fri og kritisk presse*, og at *det er væsentligt, at pressen har reel frihed til også at bringe kritiske og afslørende historier*. Vi opfordrer udvalget til at være opmærksom på, at dette ikke svækkes gennem ændringer på hverken persondatabeskyttelsesområdet eller inden for medietik og medieansvar.

Vi har bemærkninger til såvel persondataområdet som til området medieetik og -ansvar, og vi tillader os at anføre kommentarer til begge områder, uanset at høringsanmodningen alene kommer fra arbejdsgruppen vedrørende medieetik og mediansvar.

Persondataregulering
EU-Kommissionens forslag til en ny persondataregulering, fremlagt i januar 2012, indebærer, at den nye regulering skal fastsættes i en forordning, således at EU-reglerne bliver umiddelbart gældende i medlemslandene. Hvis Kommissionens forslag gennemføres, vil de nationale persondatalove blive afskaffet.

Det nuværende persondatadirektiv overlader til nationale parlamenter at fastlægge mere præcise betingelser for behandling, herunder videregivelse af persondata. Folketinget har brugt muligheden til at justere listen over sensitive oplysninger, så den passer bedre med nordisk tradition end direktivets liste. Persondataloven har desuden fået særlige regler, der begrænser brug af personoplysninger til markedsføring, og det er understreget i loven, at den ikke må anvendes i strid med informations- og ytringsfriheden ifølge Den Europæiske Menneskeretskonvention art. 10.

Kommissionens oprindelige forslag indeholder ikke en bestemmelse, der sikrer retten til aktindsigt. EU's Data Protection Supervisor har gjort opmærksom på, at persondatareguleringen kan komme i konflikt med offentlighedsregler, og han har foreslået en bestemmelse, der sikrer, at persondata ved offentlige myndigheder kan udleveres efter regler, der giver ret til aktindsigt.

Kommissionen har i forhandlinger med Rådet præsenteret et diffust forslag om "forening" af persondatabeskyttelse og retten til aktindsigt.

EU-Parlamentet har et forslag om en frist for medlemsstaterne til at meddele Kommissionen, hvilke nationale regler om aktindsigt, der kan forenes med beskyttelsen af persondata. Ingen af disse forslag sikrer retten til aktindsigt efter nationale love.

Vi opfordrer Folketinget til at overveje, om det er klogt at afskaffe de nationale lovgiveres kompetence, der hidtil er brugt i Danmark til at sikre offentlighedsregler, begrænse brug af persondata til markedsføring og til at definere oplysninger, der skal betragtes som sensitive.

Persondatareguleringens betydning for offentlighed bliver belyst af forskningschef ved Danmarks Medie- og Journalisthøjskole Oluf Jørgensen i bogen "Offentlighed i Norden", der udgives efteråret 2014 af forlaget Nordicom, Göteborgs Universitet.

Medieansvar
Det er generelt vigtigt, at virksomheder ikke kan regne med en fortjeneste ved lovovertrædelser. Det gælder også for medier, og det kan overvejes, om de nuværende retsregler giver tilstrækkelig præventiv effekt i forhold til mediers krænkelser af privatliv.

Godtgørelser til de enkelte krænkede personer kan ikke tage højde for, om der er tale om enkeltstående overtrædelse ved et medie eller gentagne, systematiske krænkelser rettet mod mange personer. Bødestraffe giver derimod mulighed for gentagelsesvirkning, og medieansvarsloven har en regel om forhold, der kan tillægges vægt ved udmåling af bøder (§ 26, stk. 2). Der er ikke en klar retspraksis om brug af denne bestemmelse. Det samme gælder for straffelovens konfiskationsregel. I den aktuelle sag har politiet rejst sigtelse mod Aller-koncernen, og politiske overvejelser om ændring af regler bør afvente udfaldet af sagen.

Se og Hør-sagen kan give anledning til at overveje retsplejelovens regler for mediers kildebeskyttelse (§ 172). Der er to undtagelser for kildebeskyttelsen. Den ene, der handler om forhold hvor strafferammen går op til 4 års fængsel, skelner ikke mellem, om anonyme kilder forsyner pressen med oplysninger om det ene eller andet. Rygter og oplysninger om privatliv er som udgangspunkt lige så beskyttede som oplysninger om samfundsmæssige forhold. Hvis samarbejdet mellem "tys-tys-kilden" og Se og Hør havde været begrænset til drypvise informationer, kunne der ikke være rejst sigtelse for forhold, der kan give op til 6 års fængsel, og kildebeskyttelsen havde været holdbar.

Den anden undtagelse for kildebeskyttelse handler om sager om overtrædelse af straffelovens tavshedspligt. I denne bestemmelse holder kildebeskyttelsen, når en journalist afdækker forhold af samfundsmæssig betydning (§ 172 stk. 6). Det kan overvejes at indsætte samme kriterium i den førstnævnte undtagelse.

Hensynet til ytringsfriheden taler stærkt for kildebeskyttelse for at sikre oplysninger om forhold, der har samfundsmæssig betydning. Der er derimod ikke væsentlige hensyn til ytringsfriheden, der taler for at beskytte kilder, der giver oplysninger om rent private forhold, uden at dette har væsentlig samfundsmæssig betydning.

Se og Hør-sagen kan i øvrigt give grund til at overveje, om denne regel om brud på tavshedspligt kun skal gælde straffelovens tavshedspligt. Den gælder for personer ved offentlige myndigheder, men ikke for personer, der udfører opgaver for private virksomheder f.eks. pengeinstitutter og NETS.

Her gælder tavshedspligt efter markedsføringsloven, men sager om brud på denne tavshedspligt kan ikke tilsidesætte kildebeskyttelse, hvis der er tale om drypvise lækager f.eks. om rent private forhold uden samfundsmæssig betydning.

I forhold til den generelle standard i danske medier har de presseetiske retningslinjer og Pressenævnet en vigtig funktion. Danske Medier og Journalistforbundet har justeret de presseetiske retningslinjer i 2013, og Pressenævnet har strammet kravene til mediers offentliggørelse af nævnets kritik.

De presseetiske krav til høring, genmæle, berigtigelser og offentliggørelse af kritik fungerer hensigtsmæssigt, og vi anser dette af større betydning for den generelle standard end eventuelle justeringer af niveauer for godtgørelser og bødestraffe. Vi anerkender dog, at niveauet af godtgørelser og bødestraffe kan have effekt i forhold til medier, der ikke lader deres varetagelse af medieetik og medieansvar påvirke af Pressenævnets sanktionssystem.

Med venlig hilsen

Jens Otto Kjær Hansen
Rektor
Danmarks Medie- og Journalisthøjskole

Folketinget
Att.: Birgitte Toft-Petersen
Christiansborg
1240 København K

Danish ICT and Electronics Federation

Vedr. høring over beretning nr. 3

DI har modtaget "Høring over beretning nr. 3" om bedre beskyttelse af personfølsomme oplysninger og effektivt tilsyn. DI takker for muligheden for at afgive bemærkninger og har i den anledning nedenstående kommentarer.

Overordnet er det af stor betydning at sikre en bedre beskyttelse af personoplysninger. Gentagne sager med tab af personoplysningers fortrolighed bidrager til at underminere tilliden til digitaliseringen. Dette har konsekvenser for såvel den offentlige som den private sektor. DI noterer sig derfor med tilfredshed, at Folketingets Kultur- og Retsudvalg har sat fokus på området.

Bredt fokus på sikkerhed

DI bakker op om, at arbejdet ikke begrænses til at kortlægge sikkerheden ved betalingskort. De tab af personoplysninger, der er sket gennem de seneste år, omfatter mange andre områder – f.eks. hacking mod kørekortregisteret, SSIs fejlagtige udlevering af sundhedsoplysninger, mange sager med fejlagtig offentliggørelse af personoplysninger i kommuner og på uddannelsesinstitutioner samt udtræk af personoplysninger fra tingbog.dk og fra bibliotekerne. Der er derfor behov for at se på, hvordan man grundlæggende kan forbedre sikkerheden ved behandling af personoplysninger i hele den offentlige sektor.

Moderne metoder og teknologier

En række moderne metoder og teknologier lover særdeles godt for at beskytte personoplysninger.

Der er for det første tale om analyse af om en given teknologisk løsning beskytter personoplysningerne godt og om oplysningerne behandling i overensstemmelse med lovens krav om formål, dataminimering, m.v. Dette kaldes en Privacy Impact Assessment (PIA). Der bør udarbejdes en skabelon for PIA, og denne bør gøres obligatorisk at anvende ved alle større offentlige it-projekter. Skabelonen bør tage udgangspunkt i, om det overhovedet er nødvendigt at identificere borgeren for at behandle vedkommendes personoplysninger, og i givet fald hvornår i behandlingsprocessen identifikation er nødvendig. Dette vil i nogle sammenhænge give

H. C. Andersens Boulevard 18
1787 København V
Danmark

(+45) 3377 3377
itek@di.dk
itek.di.dk

CVR: 16 07 75 93

en bedre beskyttelse af personoplysninger, end man kan opnå ved at anvende den skabelon for PIA, som Digitaliseringsstyrelsen har udarbejdet

For det andet bør god sikkerhed designes ind i it-løsningerne fra starten. Der bør opstilles en række helt overordnede designprincipper, som skal være grundlaget for behandling af personoplysninger. Dette kaldes Privacy by Design.

For det tredje bør der indarbejdes nye såkaldt privatlivsfremmende teknologier i de offentlige it-løsninger. Disse teknologier spænder over en bred vifte af muligheder og inkluderer i den ene ende af spektret anonymisering og pseudonymisering og i den anden ende logning og rollebaseret adgangskontrol. Der bør allerede når en løsning designes stilles krav om, at disse teknologier anvendes.

En god proces for sikker omgang med personoplysninger er derfor som følger: Man laver en analyse af, hvordan et it-system under udarbejdelse påvirker privatlivet, hvis/når der skal behandles personoplysninger. På baggrund af analysen vælges et sikkert design baseret på en gruppe af teknologier, som i særlig grad understøtter privatlivets fred. Der er behov for at disse metoder og teknologier i langt højere grad end i dag tages i anvendelse, og dette skal sikres politisk.

Persondataforordning
Lovgivning på området er en central forudsætning for at sikre en god beskyttelse af personoplysninger. Der er behov for at modernisere lovgivningen på området, som EU Kommissionen med forslaget til ny persondataforordning, har lagt op til. Der er behov for, at Danmark er langt mere imødekommende overfor EU Kommissionens forslag til persondataforordning, end det er tilfældet i dag.

For det første er det vigtigt, at forslaget bæres igennem som en forordning, der harmoniserer reglerne i Europa. Det nuværende direktiv er implementeret på 28 forskellige måder i de forskellige lande. Det betyder, at borgerne ikke kan forvente ens behandling af deres personoplysninger i Europa, og at virksomhederne skal implementere beskyttelse af personoplysninger på en ny måde, for hvert land de driver virksomhed i. De forskellige nationale implementeringer betyder også, at de europæiske nationalstater står svagere overfor at påvirke tilblivelsen af standardiserede it-løsninger. Det er en barriere overfor teknologioptag i den offentlige sektor. Hvis der var ens regler for beskyttelse af personoplysninger ville hele markedet af offentlige nationalstaters efterspørgsel kunne bidrage til at sikre optag af nye effektive teknologier med høj sikkerhed som f.eks. cloud computing.

For det andet indebærer forslaget bl.a., at der skal udarbejdes en Privacy Impact Assessment og at der arbejdes med Privacy by Design, som omtalt ovenfor. Moderne metoder og teknologier som disse kan bidrage væsentligt til at forbedre sikkerheden ved behandling af personoplysninger, hvis de implementeres korrekt. Det er derfor betydningsfuldt at bakke op bag forslaget. Der er naturligvis forhold i Kommissionens udkast, som bør justeres. DI har ved tidligere lejligheder udtalt sig mere detaljeret om forslaget til Forordning til bl.a. Folketingets Europaudvalg, og DI henviser til mere detaljerede bemærkninger i disse henvendelser.

Tilsyn
Der findes flere forskellige tilsyn på sikkerhedsområdet. Datatilsynet fører tilsyn med behandling af personoplysninger efter Lov om behandling af personoplysninger, Finanstilsynet fører tilsyn med behandling og videregivelse af personoplysninger i den finansielle sektor, Tilsynet med Efterretningstjenesterne fører tilsyn med FE og PETs behandling af personoplysninger, osv.

Man kan ikke opnå god sikkerhed alene gennem tilsyn. Men især Datatilsynet synes at kunne have behov for en styrkelse. Sagsomfanget er i takt med digitaliseringen steget betydeligt. Det er mængden af nye teknologier, som behandler personoplysninger også. Desuden er mange af teknologierne globalt interdependente, hvad der gør det vanskeligt at skabe sig overblik. Der er behov for bedre rådgivning i form af offentliggørelse af principielle vurderinger af nye teknologier – både teknologier som bruges til behandling af personoplysninger og teknologier, som bruges til at understøtte bedre sikkerhed. Sådanne vurderinger kunne både den offentlige og den private sektor drage fordel af. Styrkelsen af Datatilsynet bør således især ske på den tekniske front.

ISO27000 er et godt framework til at opnå god sikkerhed. Der findes så vidt vides ikke nogen myndighed, der fører tilsyn med implementering af god sikkerhed, herunder efterlevelse af sikkerhedsstandarden ISO27000. Rigsrevisionen påtager sig dog med mellemrum at foretage stikprøver på området. Der er behov for, at der føres et mere systematisk tilsyn med at den offentlige sektor - og dens leverandører - efterlever ISO27000. Der ville være større sandsynlighed for, at Se og Hør-sagen kunne være undgået eller i hvert fald fået et mindre omfang, hvis man havde efterlevet sikkerhedskrav som f.eks. personalegodkendelse, dataklassifikation, adgangskontrol, kryptering, logning, funktionsadskillelse og pseudonymisering. Den offentlige sektor og dens leverandører bør finde et passende niveau for implementering af relevante korrigerende sikkerhedsforanstaltninger og kontroller på baggrund af en risikovurdering.

Det vil være nyttigt, hvis der afleveres en årlig redegørelse i form af en kortlægning af sikkerhedsniveauet i den offentlige sektor til Folketinget.

Rådet for Digital Sikkerhed
DI har gennem mange år anset det for vigtigt, at der findes et uafhængigt Råd, som bidrager til både den folkelige og den faglige debat om informationssikkerhed og privacy. DI har deltaget i de forskellige offentlige Råd og Komiteer under de daværende forskningsministre. Vi har nu, hvor sådanne ikke findes længere, været med til at stifte Rådet for Digital Sikkerhed.

Rådet for Digital Sikkerhed har bidraget meget væsentligt til debatten med høringssvar, selvstændige faglige udspil, m.v. Rådet kører imidlertid med frivillige kræfter. Det er ikke sikkert, at det kan fortsætte sådan. Rådet ville desuden kunne være endnu mere aktivt, hvis Rådet havde et sekretariat. DI foreslår, at Rådet får en mindre bevilling på Finansloven til at udføre sit arbejde – f.eks. kr. 2 millioner p.a. de næste fem år. Tanken er, at Rådet til den tid vil kunne selvfinansiere et sekretariat gennem medlemskontingenter.

Viden og awareness om sikkerhed
Der bør hos alle parter i samfundet arbejdes på at forøge viden og awareness om informationssikkerhed og privacy. For det første bør der på de forskellige niveauer i uddannelsessystemet tilvejebringes viden om informationssikkerhed i takt med, at borgerne møder forskellige it-systemer. For det andet bør der over for borgerne i almindelighed tilvejebringes informationer om sikkerhed. Endelig bør der tilvejebringes informationer om, hvordan man overordnet arbejder med at skabe en sikkerhedskultur i organisationer.

Arbejdsgruppe
DI noterer sig, at Retsudvalget ønsker at nedsætte en arbejdsgruppe med inddragelse af eksterne eksperter. Det er vigtigt, at Retsudvalget lægger vægt på at arbejdsgruppen kommer med forslag, som indebærer moderne teknologier og metoder til understøttelse af sikker behandling af personoplysninger. I forhold til det udspil, Udvalget har skitseret, synes der behov for at styrke de tekniske eksterne kompetencer.

DI har utallige gange gennem de sidste seks år argumenteret for en styrkelse af sikkerheden på den tekniske front. Anvendelse af moderne teknologier og metoder, kombineret med kravene i Lov om behandling af personoplysninger, kombineret med kravene i ISO27000 og kontrolleret af en stærk myndighed er løsningen. DI har udgivet en række vejledninger, debatoplæg og høringssvar på dette område. DI stiller sig meget gerne til rådighed for en sådan arbejdsgruppe.

Semantik
Som et lille kuriosum kan det tilføjes, at Beretningen anvender en ikke helt konsistent sprogbrug. Der tales om både personoplysningslov og persondatalov, når der formodentlig refereres til samme lov. Desuden tales i Beretningen om personfølsomme oplysninger. I Lov om behandling af personoplysninger tales der derimod om almindelige, følsomme eller fortrolige personoplysninger og ikke om personfølsomme oplysninger. Det må antages, at Retsudvalget ønsker at beskytte både de følsomme og de fortrolige personoplysninger.

DI ITEK står til naturligvis til rådighed for en uddybelse af ovenstående synspunkter.

Med venlig hilsen

Henning Mortensen
Chefkonsulent
DI ITEK

Adam Lebech
Branchedirektør
DI ITEK

Folketinget
Att. Birgitte Toft-Petersen
Christiansborg
1240 København K

25. august 2014

Vedr. Høring over beretning nr. 3

Afdækning af aktuel Se & Hør sag
DANSK IT støtter, at den aktuelle sag med Se & Hør og Nets/underleverandør bliver afdækket. Ligeledes støtter DANSK IT, at regeringen skal arbejde aktivt for, at arbejdet med det kommende EU-direktiv/forordning bliver vægtet højt.

Anvendelse af fælles standard for informationssikkerhed
I forhold til den brede afdækning af datasikkerhed, som skal inddrage tekniske eksperter, kan DANSK IT tilbyde ekspertbistand. I den forbindelse ser DANSK IT også gerne, at arbejdsgruppen undersøger, hvorvidt private virksomheder og hele den offentlige sektor bør anvende fælles informationssikkerhedsstandard. I den statslige sektor er det i dag obligatorisk at anvende den internationale informationssikkerhedsstandard ISO27001, og udvalget bør overveje, om standarden kan bredes ud til andre dele af samfundet.

Ved anvendelse af ISO27001 skal informationsaktiver identificeres, og der kan gennemføres informationsklassifikation. Informationsklassifikation skal dog følges af et sikkerhedsniveau, der afspejler virksomhedes risikoprofil. Ved anvendelse af ISO27001 vil der skulle foreligge en ledelsesgodkendt risikovurdering, som en ekstern eller intern revision kan anvende som grundlag til at vurdere, om de væsentligste risici er adresseret, og om sikringstiltagene passer til de identificerede risici.

Som et led i informationsklassifikationen bør der desuden foretages konsekvensanalyser a la ”Privacy Impact Assessments”, hvor dette giver mening.

Øgede ressourcer til Datatilsynet
DANSK IT støtter, at Datatilsynet bliver styrket, så behandling af sager heri ikke er forsinkende for virksomhederne.

Med venlig hilsen

Torben Jørgensen
Formand, DANSK IT’s IT-sikkerhedsfagråd

DANSK KREDIT RÅD

Folketinget
Retsudvalget

Att.: Birgitte Toft-Petersen

Sendt per e-mail til:
Birgitte.Toft-Petersen@ft.dk

Vallensbæk Strand, 14. august 2014

Høring over 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

Dansk Kredit Råd takker for modtagelsen af høringsbrevet.

Dansk Kredit Råd har ikke kommentarer til beretningen.

Med venlig hilsen

Jacob Skriver Frandsen

Dansk Kredit Råd
Tlf.: +45 39 13 16 72
E-mail: jsf@n-cf.dk

DANSKE MEDIER

Pressens Hus
Skindergade 7
DK-1159 København K

Telefon 3397 4000
Telefax 3314 2325

info@danskemedier.dk
www.danskemedier.dk

Folketingets Retsudvalg og Kulturudvalg
Att.: Birgitte Toft-Petersen
Christiansborg
1240 København K

Sendt pr. email til Birgitte.Toft-Petersen@ft.dk

28. august 2014

Høringssvar vedr. Retsudvalgets og Kulturudvalgets beretning nr. 3

Danske Medier har modtaget ovennævnte beretning i høring fra såvel arbejdsgruppen vedrørende datasikkerhed under Retsudvalget som arbejdsgruppen vedrørende medieetik og medieansvar under Kulturudvalget. Foreningen har for overskuelighedens skyld udarbejdet nærværende samlede høringssvar, der hermed sendes til begge arbejdsgrupper.

Danske Medier er opmærksom på, at den såkaldte Se og Hør-sag er den direkte anledning til folketingsudvalgenes beretning, men foreningen er enig i, at det er relevant at belyse en række generelle spørgsmål om datasikkerhed.

Foreningen konstaterer samtidig med stor tilfredshed udvalgenes bemærkning om, at det danske demokrati blandt andet bygger på en fri og kritisk presse samt væsentligheden af pressens reelle frihed til at bringe kritiske og afslørende historier, herunder historier om magthaverne. Sidstnævnte understreger efter Danske Mediers opfattelse også helt generelt betydningen af den grundlovssikrede tredeling af magten, der forhindrer den udøvende magt i at have indflydelse på domstolenes bedømmelse af ytringsfrihedens grænser.

Danske Medier har følgende konkrete bemærkninger til beretningen:

Arbejdsgruppen vedrørende datasikkerhed

Danske Medier finder det meget positivt, at udvalgene i beretningen anerkender værdien af "kommerciel udnyttelse af big data", og at det understreges, at brugen af store datasæt er legitim, så længe data ikke kan føres tilbage til identificerede enkeltpersoner.

Foreningen bifalder derfor også, at arbejdsgruppen vedrørende datasikkerhed skal se på erfaringen med anonymisering af data. Danske Medier foreslår i den forbindelse, at arbejdsgruppen tilføres ekstern ekspertise inden for netop "big data".

Arbejdsgruppen vedrørende medieetik og medieansvar

Danske Medier noterer, at arbejdsgruppen vedrørende medieetik og medieansvar forventes i hvert tilfælde at behandle spørgsmål om erstatningsansvar ved freds- og ærekrænkelser, mediers brug af betalte kilder samt praksis og normalstrafniveau i sager om publicering af "urigtige historier".

For så vidt angår erstatningsansvar henholder Danske Medier sig til Justitsministeriets redegørelse om niveauet for økonomisk kompensation til ofre for urigtige historier i medierne.[1] Det konkluderes heri, at Justitsministeriet ikke finder, at der "aktuelt er anledning til at gennemføre lovgivning med det sigte at foretage en forhøjelse af kompensationsniveauet i forhold til sager om ærekrænkelser mv., særligt for så vidt angår sager om urigtige historier, der bringes i medierne."

Danske Medier tager klar afstand fra kontinuerlig betaling af kilder, således som det angiveligt er sket i den såkaldte Se og Hør-sag. Foreningen finder i øvrigt, at tiphonorering og betalte kilder er det enkelte medies sag, men at mediet med fordel kan offentliggøre sine retningslinjer herfor. Det kan ikke udelukkes, at der kan være situationer, hvor betaling af kilder kan få historier af væsentlig samfundsmæssig betydning frem. Danske Medier har dog ikke kendskab til konkrete eksempler herpå, og det er i øvrigt foreningens vurdering, at betaling af kilder ikke har nogen nævneværdig udbredelse blandt danske medier. For fuldstændighedens skyld skal det endelig bemærkes, at betaling i nogle tilfælde også dækker det ophavsretlige vederlag, der tilkommer en kilde ved overdragelse af fx billedmateriale til brug for publicering.

Danske Medier bifalder udvalgenes ønske om en gennemgang af praksis og normalstrafniveau over for medier i forbindelse med publicering af urigtige historier, idet foreningen dog samtidig konstaterer, at det af Justitsministeriets ovenfor nævnte redegørelse fremgår, at den tilgængelige retspraksis om urigtige historier i medierne er begrænset. Foreningen opfordrer i den forbindelse til, at det tydeliggøres, hvad der menes med "urigtige historier", idet freds- og ærekrænkelser ofte vedrører sande historier. Danske Medier finder det naturligt, at Justitsministeriet inddrages i denne praksisgennemgang.

Foreningen er opmærksom på, at arbejdsgruppen skal afrapportere til Kulturudvalget. Da de ovenfor nævnte emner ifølge beretningen forventes behandlet i samarbejde med pressens repræsentanter, beder Danske Medier venligst om at få lejlighed til at kommentere arbejdsgruppens konklusioner forud for denne afrapportering.

Danske Medier ser i øvrigt frem til det planlagte dialogmøde med arbejdsgruppen om medieetik og medieansvar 10. september 2014. Foreningen står naturligvis også til rådighed, såfremt ovenstående allerede før dialogmødet giver anledning til spørgsmål.

[1] Kulturudvalget, Alm. del 2013-14 bilag 152, som berigtiget i bilag 153

Henvendelser herom kan rettes til adm. direktør Ebbe Dal på telefon 3397 4000 eller ed@danskemedier.dk.

Med venlig hilsen
Danske Medier

Ebbe Dal
Adm. direktør

Folketingets Retsudvalg
Att.: Birgitte Toft-Petersen

DANSKE REGIONER

29-08-2014
Sag nr. 14/2255
Dokument 44378/14
Katrine Stokholm
kst@regioner.dk

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.

Det er afgørende, at borgerne har tillid til, at der fuld fortrolighed om deres personfølsomme oplysninger. Her er der særligt behov for, at borgerne fortsat har tillid til håndteringen af personfølsomme data i kommuner, regioner og staten.

Danske Regioners mener, at den eksisterende lovgivning er tilstrækkelig til at sikre fortrolighed om personfølsomme oplysninger. Udfordringen er således at styrke håndhævelsen af den gældende lovgivning. Danske Regioner finder ikke, at der er behov for et strammere regelsæt på området.

Endvidere er det Danske Regioners vurdering, at der ikke er behov for at ændre på den danske linje i forhold til arbejdet med en ny EU-direktiv/forordning om persondatabeskyttelse. Der bør som hidtil arbejdes for, at der kan udveksles relevante data om patienter mellem behandlende parter inden for sundhedsvæsenet. Endvidere bør der som hidtil være mulighed for at gennemføre forskning under løbende kontrol fra Datatilsynet.

Danske Regioner vil understrege vigtigheden af at have en nuanceret drøftelse af datasikkerhed. Datasikkerhed går på tværs af politik- og ressortområder. Løsningerne skal tage højde for, at brug af data en forudsætning for kommunale og regionale kerneopgaver. Endvidere er data en forudsætning for at generere ny viden samt skabe innovation og vækst, herunder nye og bedre behandlingsformer i sundhedsvæsenet.

Dampfærgevej 22
Postboks 2593
2100 København Ø

T 35 29 81 00
F 35 29 83 00
E regioner@regioner.dk

Arbejdsgruppens afdækning af datasikkerhed bør derfor tage højde for, at udveksling af valide og relevante data understøtter en række væsentlige velfærdsydelser.

Personfølsomme oplysninger er ikke alene reguleret af logningsreglerne og persondataloven, men også af en lang række andre love. Denne kompleksitet skal også reflekteres i overvejelserne om, hvorvidt der er behov for en samling af it- og datasikkerhed ved en ansvarlig ressortminister. Endelig bør det overvejes, hvordan borgerne informeres i tilfælde af sikkerhedsbrud.

Udveksling af relevante data om den enkelte patient mellem hospital, hjemmeplejen og den praktiserende læge er en forudsætning for god og sikker patientbehandling på tværs af sektorer. I fremtiden vil stadig flere patienter blive udskrevet fra hospitalet til videre behandling og pleje i kommunerne, og der vil dermed blive et stigende behov for at dele relevante data. Denne deling af data er en forudsætning for implementering af flere dele af den fællesoffentlige digitaliseringsstrategi.

Det er positivt, at mulighederne for at anonymisere data undersøges og konkretiseres. Anonymisering af data ville kunne sikre en enklere adgang til data til forskning og kvalitetsudvikling. Endvidere er en årlig redegørelse om datasikkerhed samt om en drøftelse af pressens repræsentanter til en drøftelse af de medieetiske regler konstruktive tiltag, der kan understøtte en bedre sikkerhed om borgernes personfølsomme oplysninger.

Det er fornuftigt at iværksætte en nærmere undersøgelse af, hvorvidt der skal være en obligatorisk databeskyttelsesvurdering i digitale projekter. Det bør dog overvejes, om det samme skal være tilfældet for den private sektor. Endvidere bør der tages forbehold for de økonomiske konsekvenser for kommuner og regioner, såfremt der pålægges nye opgaver.

Det er positivt, at tekniske eksperter inddrages i arbejdsgrupperne. Der bør dog også inddrages repræsentanter fra de interessenter, der bruger data. Relevante og valide data er en forudsætning for en god og effektiv opgaveløsning i kommuner og regioner. Endvidere er adgangen til data nødvendig for at sikre udvikling af velfærdsydelser. Derfor bør blandt andet Danske Regioner, KL samt repræsentanter for forskning mv. være repræsenteret i arbejdsgruppen. Datatilsynet bør også inddrages, da de har erfaringerne med håndhævelse af den aktuelle lovgivning.

Med venlig hilsen

Tommy Kjelsgaard

DATATILSYNET

Folketinget
Udvalgssekretariatet
Christiansborg
1240 København K

Sendt til: Birgitte.Toft-Petersen@ft.dk

29. august 2014

Datatilsynet
Borgergade 28, 5.
1300 København K

CVR-nr. 11-88-37-29

Telefon 3319 3200
Fax 3319 3218

E-mail
dt@datatilsynet.dk
www.datatilsynet.dk

J.nr. 2014-19-0041
Sagsbehandler
Maiken Christensen
Direkte 3319 3224

Vedrørende høring over beretning nr. 3

1. I e-mails af 26. juni 2014 har arbejdsgruppen vedrørende medieetik og medieansvar under Folketingets Kulturudvalg samt arbejdsgruppen om datasikkerhed under Folketingets Retsudvalg anmodet om bemærkninger til beretning nr. 3 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".

2. I den anledning kan Datatilsynet oplyse følgende:

2.1. Det fremgår af beretningen, at arbejdsgruppen vedrørende datasikkerhed under Folketingets Retsudvalg konkret forventes at se på bl.a. eksternt tilsyn med overholdelse af gældende lovgivning, herunder Datatilsynets kompetencer og ressourcer, samt andre tilsynsorganer af relevans for området og behovet for eventuel oprettelse af nye organer.

Datatilsynet skal bemærke, at tilsynets opgavevaretagelse og medarbejdersammensætning i høj grad afspejler den lovgivning, der findes på området for persondatabeskyttelse. Således er langt størstedelen af tilsynets opgaver i dag lovbundne.

Datatilsynet har bl.a. følgende opgaver og funktioner:

- Generel vejledning og rådgivning af offentlige myndigheder og private vedrørende behandling af oplysninger
- Behandling af klagesager og sager, der tages op af egen drift
- Behandling af anmeldelser fra offentlige myndigheder, der behandler fortrolige oplysninger
- Behandling af ansøgninger om tilladelse fra private virksomheder mv., der behandler følsomme oplysninger
- Behandling af ansøgninger fra private virksomheder mv. om tilladelse til behandling af oplysninger i forbindelse med stillingsbesættende virksomhed, kreditoplysningsvirksomhed, advarselsregistre og retsinformationssystemer
- Behandling af ansøgninger om tilladelse til overførsel af oplysninger til tredjelande

- Udførelse af inspektioner hos offentlige myndigheder, private virksomheder, forskere mv.
- Afgivelse af udtalelse ved udarbejdelsen af bekendtgørelser, cirkulærer eller lignende generelle retsforskrifter, der har betydning for beskyttelsen af privatlivet i forbindelse med behandling af personoplysninger
- Nationalt tilsyn med internationale informationssystemer, f.eks. den nationale del af Schengen Informationssystemet (SIS)
- Deltagelse i internationalt samarbejde, f.eks. i de fælles tilsynsmyndigheder nedsat i henhold til Schengen- og Europolkonventionerne og i EU-regi

Herudover har Datatilsynet opgaver i henhold til anden lovgivning. F.eks. modtager tilsynet anmeldelser i henhold til lov om massemediers informationsdatabaser. Endvidere er Datatilsynet Registertilsyn for Grønland og i forhold til rigsmyndighederne på Færøerne i medfør af de dér gældende registerlove.

Datatilsynet skal pege på, at overvejelser om en styrkelse af Datatilsynet ikke alene bør fokusere på omfanget af ressourcer, men også på indholdet af de opgaver, som Datatilsynet forventes at varetage.

Det kan f.eks. overvejes, om tilsynet fortsat i samme udstrækning som i dag skal udstede tilladelser til virksomheder, der behandler oplysninger, samt behandle anmeldelser fra offentlige myndigheder, der behandler fortrolige oplysninger som naturlig følge af deres myndighedsudøvelse.

Datatilsynet skal i øvrigt bemærke, at tilsynet udøver sine funktioner i fuld uafhængighed, jf. persondatalovens[1] § 56. Bestemmelsen har sin baggrund i databeskyttelsesdirektivets[2] artikel 28, stk. 1, 2. afsnit.

2.2. Af beretningen fremgår endvidere, at arbejdsgruppen vedrørende datasikkerhed under Folketingets Retsudvalg konkret forventes at se på bl.a.

- internt tilsyn, herunder sikkerhedsgodkendelse af personer med adgang til personfølsomme data, samt opdeling af medarbejdere i flere sikkerhedsniveauer, der regulerer adgangen til oplysninger
- muligheden for at stille yderligere krav til både offentlige og private dataansvarlige, herunder anvendelse af privacy by design, logning af opslag i registre, forbud mod unødvendig sammenkøring af oplysninger og lign.

Datatilsynet skal i den forbindelse bemærke, at for *offentlige myndigheder* er persondatalovens sikkerhedskrav nærmere udmøntet i sikkerhedsbekendtgørelsen[3] og sikkerhedsvejledningen[4].

---

[1] Lov nr. 429 af 31. maj 2000 om behandling af personoplysninger med senere ændringer

[2] 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

Sikkerhedskravene for offentlige myndigheder omfatter – afhængigt af den konkrete behandling af personoplysninger – navnlig følgende:

- forpligtelsen til at fastsætte nærmere retningslinjer, der beskriver, hvordan de fornødne sikkerhedsforanstaltninger konkret er etableret i organisationen,
- kravet om instruktion af medarbejderne,
- kravet om skriftlige aftaler med eventuelle databehandlere til sikring af, at datasikkerheden lever op til persondataloven og sikkerhedsbekendtgørelsen, samt at den dataansvarlige påser dette,
- kravet om særlige retningslinjer ved adgang til personoplysninger ved brug af it-udstyr uden for den dataansvarliges lokaliteter (hjemmearbejdspladser og lign.),
- kravet om fysisk sikkerhed
- kravet om iagttagelse af de fornødne sikkerhedsforanstaltninger i forbindelse med reparation og service samt ved salg og kassation af anvendte datamedier,
- kravet om formel autorisationsprocedure, der sikrer, at kun personer, som autoriseres hertil, har adgang til personoplysninger, og at der kun autoriseres personer, for hvem adgangen er nødvendig som led i deres jobfunktion, at disse tildeles et individuelt personligt login, samt at den udstedte autorisation ændres eller lukkes ved medarbejderens fratræden eller flytning inden for organisationen,
- kravene om, at der ved transmission via internettet (eller andre åbne net) foretages en risikovurdering omfattende alle elementer i løsningen, at der implementeres de fornødne sikkerhedsforanstaltninger til imødegåelse af de foreliggende risici, herunder brug af kryptering, hvis fortrolige eller følsomme personoplysninger overføres via internettet (eller andre åbne net), og om sikring af sikkerhed for autenticitet (afsenders og modtagers identitet) og integritet (de transmitterede oplysningers ægthed) i fornødent omfang ved anvendelse af passende sikkerhedsforanstaltninger,
- kravet om kontrol med afviste adgangsforsøg, herunder blokering for yderligere forsøg efter et antal afviste adgangsforsøg samt
- kravet om registrering (logning) af alle anvendelser af personoplysninger.

I den *private sektor* er der ikke på samme måde fastsat mere præcise regler om behandlingssikkerheden. For den private sektor gælder derfor rammebestemmelsen i persondatalovens § 41, stk. 3.

Af denne bestemmelse fremgår, at den dataansvarlige skal træffe de fornødne tekniske og organisatoriske sikkerhedsforanstaltninger mod, at oplysninger

---

[3] Justitsministeriets bekendtgørelse nr. 528 af 15. juni 2000, som ændret ved bekendtgørelse nr. 201 af 22. marts 2001, om sikkerhedsforanstaltninger til beskyttelse af personoplysninger, som behandles for den offentlige forvaltning

[4] Datatilsynets vejledning nr. 37 af 2. april 2001 til bekendtgørelse nr. 528 af 15. juni 2000 om sikkerhedsforanstaltninger til beskyttelse af personoplysninger, som behandles for den offentlige forvaltning

hændeligt eller ulovligt tilintetgøres, fortabes eller forringes samt mod, at de kommer til uvedkommendes kendskab, misbruges eller i øvrigt behandles i strid med loven. Tilsvarende gælder for databehandlere.

Datatilsynet kan dog i forbindelse med udstedelse af tilladelser til behandling af personoplysninger hos private virksomheder mv. stille krav om, at der træffes konkrete sikkerhedsforanstaltninger. Det kan f.eks. være krav om autorisation og adgangskontrol og i enkelte tilfælde om registrering (logning) af alle anvendelser af personoplysninger.

Datatilsynet har endvidere på visse områder fastsat egentlige krav til datasikkerheden i den private sektor. Det gælder bl.a. ved overførsel af følsomme oplysninger via hjemmesider, hvor tilsynet stiller krav om kryptering.

2.3. Vedrørende den konkrete sag, der har givet anledning til nedsættelsen af arbejdsgrupperne, kan det oplyses, at Datatilsynet af egen drift har iværksat flere undersøgelser.

Datatilsynet blev via presseomtale den 28. april 2014 bekendt med, at Se og Hør angiveligt systematisk skulle have indsamlet og brugt oplysninger fra Nets (tidligere PBS) om kendte danskeres brug af kreditkort. Datatilsynet anmodede samme dag Se og Hør om en redegørelse til brug for tilsynets overvejelser om, i hvilket omfang der kan have været tale om behandling af personoplysninger i strid med persondataloven. Datatilsynet gjorde samtidig opmærksom på, at Se og Hør ikke var forpligtet til at afgive oplysninger, idet der kunne være risiko for, at der blev afgivet oplysninger om, at der var begået noget strafbart.

Aller Media A/S besvarede ved brev af 15. juli 2014 Datatilsynets henvendelse. Aller Media A/S oplyste, at Aller Media A/S er sigtet af politiet og derfor ikke ønsker at udtale sig til tilsynet.

På den baggrund har Datatilsynet oversendt sagen til Københavns Vestegns Politi med anmodning om, at spørgsmålet om eventuel overtrædelse af persondataloven i stedet inddraget i politiets sag mod Aller Media A/S.

Tilsynet har ligeledes af egen drift iværksat undersøgelser af SAS og Rigshospitalet (Region Hovedstaden), idet det af medieomtale er fremgået, at Se og Hør fra medarbejdere hos SAS og Rigshospitalet skal have modtaget oplysninger om kendte personer.

Sagerne vedrørende Rigshospitalet og SAS er på nuværende tidspunkt endnu ikke afsluttede hos Datatilsynet.

Det bemærkes, at Datatilsynet er bekendt med, at Finanstilsynet undersøger forholdene hos Nets og i den forbindelse har indhentet en redegørelse fra Nets. På den baggrund har Datatilsynet på nuværende tidspunkt ikke iværksat en selvstændig undersøgelse af Nets.

Se og Hør-sagen har i øvrigt affødt en henvendelse til Datatilsynet fra Danske Medier om mediernes anmeldelse til tilsynet af redaktionelle informationsdatabaser, ligesom tilsynet har modtaget et stort antal af sådanne anmeldelser fra danske massemedier.

2.4. Datatilsynet skal afslutningsvis bemærke, at der i beretningen flere gange anvendes begrebet "personfølsomme oplysninger".

Datatilsynet kan i den forbindelse oplyse, at begrebet "personfølsomme oplysninger" ikke anvendes i persondataloven eller i tilsynets praksis.

I persondataloven findes begrebet "personoplysninger". Det dækker alle typer af oplysninger om personer, både følsomme og ikke-følsomme oplysninger.

Følsomme oplysninger er de oplysninger, som er nævnt i persondatalovens §§ 7-8, herunder f.eks. helbredsoplysninger og oplysninger om strafbare forhold. En betalingsoplysning vil normalt ikke være en følsom oplysning, men vil som udgangspunkt være omfattet af reglerne i lovens § 6 om almindelige ikke-følsomme oplysninger.

Personnummer er heller ikke en følsom oplysning efter persondataloven, men det er en oplysning, der nyder en særlig beskyttelse efter persondatalovens § 11.

Datatilsynet skal på den baggrund foreslå, at der i arbejdsgruppernes videre arbejde – bl.a. for at undgå tvivlsspørgsmål i relation til persondataloven – anvendes en terminologi svarende til persondatalovens, herunder at der som overordnet begreb anvendes betegnelsen "personoplysninger".

3. Datatilsynet står naturligvis til rådighed, hvis det videre arbejde skulle give anledning til konkrete spørgsmål af persondataretlig karakter eller spørgsmål om tilsynets virksomhed.

Med venlig hilsen

Birgit Kleis
Kst. direktør

DEN DANSKE DOMMERFORENING

Dato:
- 2 JULI 2014

Folketinget
Retsudvalget
Christiansborg
1240 København K

Høringssvar er sendt pr. mail til birgitte.toft-petersen@ft.dk

Folketingets Retsudvalg har ved brev af 25. juni 2014 anmodet Dommerforeningen om eventuelle bemærkninger til beretning nr. 3 (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).

I den anledning skal jeg meddele, at beretningen ikke giver Dommerforeningen anledning til at fremkomme med bemærkninger.

Med venlig hilsen

Mikael Sjöberg

Formanden, Østre Landsret, Bredgade 59, 1260 København K, tlf. 99 68 65 01
mikaelsjoberg@oestrelandsret.dk

Domstolsstyrelsen

Folketinget
Udvalgssekretariat
Christiansborg
1240 København K

Store Kongensgade 1-3
1264 København K
Tlf. +45 70 10 33 22
post@domstolsstyrelsen.dk
CVR-nr. 21659509
EAN-nr. 5798000161184

Sendt pr. e-mail til Birgitte.Toft-Petersen@ft.dk

J.nr. 2014-4102-0023-3
Sagsbeh. Katrine Valbjørn Trebbien
kat@domstolsstyrelsen.dk
29. august 2014

Beretning nr. 3 om nedsættelse af en parlamentarisk arbejdsgruppe

Ved breve fremsendt med e-mail af 26. juni 2014 har arbejdsgruppen vedrørende medieetik og medieansvar under Folketingets Kulturudvalg og arbejdsgruppen vedrørende datasikkerhed under Folketingets Retsudvalg bedt om Domstolsstyrelsens eventuelle bemærkninger til beretning nr. 3 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.

Domstolsstyrelsen har ikke bemærkninger til beretningen.

Med venlig hilsen

Katrine Valbjørn Trebbien

Til
Folketingets Kulturudvalg og Retsudvalg,
Arbejdsgruppen vedrørende datasikkerhed under Retsudvalget

Att. Birgitte Toft-Petersen, Birgitte.Toft-Petersen@ft.dk.

29. august 2014

Finanssektorens Hus
Amaliegade 7
DK-1256 Copenhagen K

Telefon 3370 1000
Fax 3393 0260

mail@finansraadet.dk
www.finansraadet.dk

Kontakt Henriette Rolskov
Direkte +45 3370 1102
her@finansraadet.dk

Journalnr. 466/05
Dok. nr. 525521-v3

Høringssvar vedrørende beretning nr. 3

Hermed fremsendes Finansrådets høringssvar vedrørende nedsættelse af de to parlamentariske arbejdsgrupper, 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. Denne høring er modtaget af arbejdsgruppen vedrørende datasikkerhed under Retsudvalget.

Finansrådet er meget positiv ift. nedsættelsen af arbejdsgrupperne i forlængelse af "Se og Hør"-sagen. Borgernes fortsatte tillid til at deres personfølsomme oplysninger håndteres forsvarligt er en helt afgørende forudsætning for den fortsatte digitalisering. Sagen har derfor også haft den største bevågenhed hos Finansrådets medlemmer.

I forlængelse af sagen er der i Finansrådets regi nedsat en arbejdsgruppe vedrørende beskyttelse af fortrolige kundeoplysninger, hvor bankerne på sektorfælles niveau har indledt drøftelser om håndteringen af relevante regler og procedurer i sektoren og mulige fremadrettede tiltag.

Sagen behandles med største alvor, og de enkelte banker har i naturlig forlængelse af sagen vurderet egne sikkerhedsprocedurer. Finansrådet har i august 2014 orienteret Erhvervs- og Vækstministeriet om det igangværende arbejde i sektoren og de indledende overvejelser om relevante sektorinitiativer. Finansrådet vil i september 2014 give Erhvervs- og vækstministeriet en tilbagemelding på, hvad sektoren på den baggrund vil foretage sig.

It-sikkerhed er essentiel for bankerne, da det er en forudsætning for kundernes tillid, men samtidig er det også afgørende, at bankerne kan betjene kunderne og være der, når en kunde har behov for hjælp, og det kræver adgang til kundedata.

Bankerne arbejder med kontroller på mange niveauer, men det vil aldrig være muligt at gardere sig 100 procent i en ulykkelig sag som Se og Hørsagen, hvor der både er sælgere og købere, der er villige til at bryde alle regler og etiske rammer. Samtidig er det dog klart, at finanssektoren hele tiden skal gøre sit yderste for at implementere og vedligeholde kontroller, der sikrer, at borgernes personfølsomme data behandles forsvarligt. Heldigvis kan Finansrådet ikke genkende sagen som et symptom på den generelle

sikkerhedstilstand i banksektoren. Denne vurderes fortsat at være på et meget højt niveau, og der investeres fortsat mange ressourcer – både personalemæssige og økonomiske – i it-sikkerhed.

Finansrådet deler udvalgenes betragtning om, at omfanget af opgaven ikke kan begrænse sig til oplysninger om betalingskort, men bør omfatte alle områder, hvor der opbevares og behandles personfølsomme oplysninger og data.

I forhold til initiativer om yderligere regulering gør Finansrådet opmærksom på, at der allerede findes omfattende regulering af finansielle virksomheder i forhold til it-sikkerhed, herunder persondatabeskyttelse i de danske banker.

I arbejdet med initiativer efter Se og Hør-sagen, bør det sikres, at eventuelle danske initiativer er i tråd med den kommende EU- forordning på databeskyttelsesområdet, således at der ikke gennemføres nationale særinitiativer, som senere er i kontrast til den harmoniserende forordning.

Finansrådet vil gerne på sektorens vegne tilbyde at bidrage i den videre dialog vedrørende beskyttelse af følsomme/fortrolige personoplysninger, herunder inddrage de mangeårige erfaringer, bankerne har i forhold til implementering af reglerne for it-sikkerhed i finansielle virksomheder.

Med venlig hilsen

Henriette Rolskov

Direkte +45 3370 1102
her@finansraadet.dk

FORBRUGEROMBUDSMANDEN

Folketingets Udvalgssekretariat
Christiansborg
1240 København K

Att. Retsudvalget / Arbejdsgruppen om datasikkerhed og
Kulturudvalget / Arbejdsgruppen om medieansvar og medieetik

Dato: 29. august 2014

Sag: FO-14/07250-3

Sagsbehandler: /dsk

FORBRUGEROMBUDSMANDEN
Carl Jacobsens Vej 35
2500 Valby

Tlf. 41 71 51 51
Fax 41 71 51 61
CVR-nr. 10 29 48 19
EAN-nr. 5798000018006
forbrugerombudsmanden@kfst.dk
www.forbrugerombudsmanden.dk

ERHVERVS- OG VÆKSTMINISTERIET

Høring vedrørende 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

Tak for e-mails af 26. juni 2014 fra henholdsvis arbejdsgruppen om datasikkerhed under Folketingets Retsudvalg og arbejdsgruppen om medieansvar og medieetik under Folketingets Kulturudvalg, hvor udvalgenes beretning af 3. juni 2014 sendes i høring.

Forbrugerombudsmanden er enig i, at det er fornuftigt at vurdere behovet for bedre beskyttelse af personfølsomme oplysninger, og vi hilser derfor arbejdet velkomment.

Det fremgår af beretningen, at arbejdsgruppen vedrørende datasikkerhed bl.a. aktivt skal inddrage tekniske og juridiske eksperter, herunder Forbrugerombudsmanden. Vi er naturligvis indforstået med at bistå arbejdsgruppen.

Forbrugerombudsmanden deltog således i mødet i Folketinget tirsdag den 26. august 2014. For en ordens skyld gentages her de områder, hvor Forbrugerombudsmanden finder, at der kan være problemer med databeskyttelse:

- CPR-nummer afkræves ofte i forbindelse med aftaleindgåelse. Vi ser en stigning i antallet af henvendelser, hvor erhvervsdrivende afkræver CPR-nummer også i forbindelse med køb, hvor det ikke synes at være sagligt begrundet. Kan være en overtrædelse af god markedsføringsskik.
- Sager om abonnementsfælder: Tæt på en "landeplage". Pr. 13. juni 2014 skærpede regler i forbrugeraftaleloven, hvorefter det nu klart skal angives, om der er tale om et abonnement. Ellers er aftalen ikke gyldig.
- Sager om bilvurderinger: Forbrugere får regninger, selv om de har afbrudt bestillingsforløbet eller har benyttet sig af fortrydelsesretten. I øvrigt ofte en meget uklar aftaleindgåelse.

- *BIG-data* – indsamling af oplysninger om forbrugeradfærd. Informationerne kan bruges til målrettet markedsføring og behavioral pricing. Problemstillingen drøftes i de internationale fora, hvor Forbrugerombudsmanden deltager. Der bør iværksættes en EU-undersøgelse, som skal belyse denne problemstilling.
- Forbrugerombudsmandens nye retningslinjer af 1. september 2014 vedrørende E-butikkers håndtering af betalinger og kreditkortoplysninger (fortrolige data). Bl.a. krav til information, *inden* der hæves beløb på kontoen. Supplement til reglerne i betalingstjenesteloven, herunder regler om forudbetaling og efteropkrævninger.

Håndhævelse:

- Datatilsynet skal håndhæve persondataloven. Forbrugerombudsmanden håndhæver markedsføringsloven. Forudsætter et parløb.

Mulige løsninger:

- Mulighed for at lukke for adgangen til hjemmesider via fogedforbud ved åbenlyse overtrædelser af persondataloven og/eller markedsføringsloven.
- Mere effektivt internationalt samarbejde og bedre efterforskningsredskaber.
- Aftale om udveksling af fortrolige oplysninger mellem EU og USA om bl.a., hvem der er ansvarlig for hjemmesider.
- Revision af e-handelsdirektivet fra 2000 om bl.a. kompetencespørgsmål og ansvarsfrihed. Der er sket meget de seneste 14 år på de elektroniske medier.

Folketingets Retsudvalg har tidligere bedt Forbrugerombudsmanden om at fremsende forslag til mulige initiativer, som kunne sikre en bedre håndhævelse af international bekæmpelse af svindel på nettet. Der vedlægges kopi af disse forslag.

Med venlig hilsen
På Forbrugerombudsmandens vegne

Diane Svanholm Kvist
Procedør, specialkonsulent

FORBRUGEROMBUDSMANDEN

NOTAT

Dato: 14. maj 2014

Sag: FO-14/03722-5

Sagsbehandler: /kn

Forslag til tiltag, der kan forbedre den internationale håndhævelse inden for det forbrugerretlige område – Forbrugerombudsmandens oplæg på møde den 3. april 2014 i Folketingets Retsudvalg

I forbindelse med Forbrugerombudsmandens oplæg om international bekæmpelse af svindel på internettet på mødet den 3. april 2014 med Folketingets Retsudvalg anmodede medlemmer af Retsudvalget Forbrugerombudsmanden om at uddybe, hvor man navnlig kan styrke håndhævelsen.

Forbrugerombudsmanden fremsender derfor hermed en kort oversigt over områder, hvor der er behov for bedre rammer for håndhævelsen af grænseoverskridende overtrædelser af den forbrugerbeskyttende lovgivning.

Forbrugerombudsmanden står gerne til rådighed for at nærmere uddybning af punkterne, såfremt Folketinget Retsudvalg måtte ønske det.

1. Mulighed for at lukke adgangen til hjemmesider

Mange overtrædelser foregår fra hjemmesider, hvor udbyderne er etableret i lande uden for EU. I disse sager er det umuligt både for Forbrugerombudsmanden og andre myndigheder - herunder politiet – at få stoppet overtrædelserne. Det vil derfor være hensigtsmæssigt, hvis det blev muligt fra Danmark at blokere for disse hjemmesider. Spillemyndigheden har siden den 1. januar 2012 i henhold til spilleloven[1] haft en sådan adgang til via en retskendelse at blokere for hjemmesider med ulovligt indhold. Et sådant tiltag skal naturligvis balanceres over for hensynet til ytringsfriheden og skal derfor kun benyttes, såfremt andre håndhævelsesskridt har vist sig forgæves. Det vil imidlertid være en væsentlig hjælp til bekæmpelse af den grænseoverskridende svindel på internettet.

2. Ansvarsfrihedsreglerne på internettet

Efter E-handelsloven[2], der bygger på E-handelsdirektivet[3], er en udbyder af en hosting-tjenesteydelse ikke ansvarlig for det indhold, som andre

[1] Lov nr. 848 af 1. juli 2010 med senere ændringer.
[2] Lov nr. 227 af 22. april 2002.
[3] Europa-Parlamentets og Rådets direktiv 2000/31/EF.

lægger ud på hjemmesiden. Dette indebærer, at fx en søgemaskinehjemmeside eller et socialt medie ikke kan gøres ansvarlig for overtrædelser, der foregår på deres hjemmesider. Reglerne stammer fra en tid før udbredelsen af de sociale medier, som i højere grad end tidligere internettjenesteudbydere styrer den kommercielle kommunikation, der foregår på deres platforme. Lovens regler om ansvarsfrihed er derfor utidssvarende. Internettjenesteudbydere – så som sociale medier - bør tage aktiv del i bekæmpelsen af den svindel, der foregår på deres hjemmesider og bør kunne holdes ansvarlig. Der bør derfor arbejdes på, at der sker en revision af reglerne om ansvarsfrihed på internettet i EU.

3. Definitionen på spam

Ligeledes er også beskyttelsen mod spam utidssvarende i forhold til den teknologiske udvikling. Markedsføringslovens § 6[4], der forbyder udsendelse af spam, baserer sig på en forældet definition af, hvad der er elektronisk post og dermed spam og omfatter fx ikke den markedsføring, som man i stigende grad udsættes for på de sociale medier. Idet denne regel ligeledes bygger på EU lovgivning rettede de nordiske forbrugerombudsmænd den 3. maj 2012 henvendelse til EU-Kommissionen med henblik på, at få definitionen revideret. Brevet til EU-Kommissæren og dennes svar vedlægges til orientering. Der er endnu ikke sket noget, hvorfor der også her bør arbejdes på at få reglerne ændret i EU.

4. Det europæiske håndhævelsessamarbejde

Forbrugerombudsmanden deltager i det internationale CPC håndhævelsessamarbejde inden for EU under den såkaldte håndhævelsesforordning[5]. Inden for dette samarbejde kan en myndighed i et medlemsland anmode et andet medlemsland om at tage skridt til at stoppe en grænseoverskridende overtrædelse, hvis den foretages af en virksomhed som er hjemmehørende i dette medlemsland. Der mangler imidlertid mulighed for at kunne gribe ind, hvis det medlemsland, hvor virksomheden er hjemmehørende, ikke foretager sig noget. Endvidere bør der være en bedre mulighed for at udveksle fortrolige oplysninger mellem de forskellige landes håndhævelsessamarbejde, og man bør kunne offentliggøre oplysninger om de sager, der indgår i dette regi. Reglerne bør derfor ændres, så der skabes bedre rammer for håndhævelsessamarbejdet i EU.

[4] Lovbekendtgørelse nr. 1216 af 25. september 2013 med senere ændringer.
[5] Europa-Parlamentets og Rådets forordning nr. 2006/2004.

5. Det internationale håndhævelsessamarbejde

Relationerne til de relevante internationale myndigheder bør styrkes. Navnlig bør adgangen til at kunne samarbejde med de amerikanske myndigheder om grænseskrivende svindel på internettet forbedres, da en del virksomheder, der overtræder EU-reglerne, er etableret i USA. Det bør være muligt at udveksle fortrolige oplysninger og at søge bistand fra de amerikanske myndigheder. I EU har der i nogen tid været arbejdet på en samarbejdsaftale med de amerikanske myndigheder, men dette har endnu ikke ført til konkrete tiltag. Der bør derfor fortsat arbejdes for dette inden for EU.

6. Revision af markedsføringsloven

Det bør overvejes, om der bør ske en grundig revision af markedsføringslovens regler, således at den i struktur og indhold stemmer bedre i overensstemmelse med direktivet om urimelig handelspraksis[6]. Dette vil gøre håndhævelsen af grænseoverskridende overtrædelser lettere.

[6] Europa-Parlamentets og Rådets direktiv 2005/29/EF.

Fiolstræde 17 B, Postboks 2188, 1017 København K
T: +45 7741 7741, F: +45 7741 7742, fbr@fbr.dk, taenk.dk

Folketingets Retsudvalg
Sendt pr. e-mail til Birgitte Toft-Petersen

29-08-2014
Dok. 143340/ah

Beretning 3: Bedre beskyttelse af personoplysninger og et effektivt tilsyn med offentlige og private virksomheder.

Med henvisning til Folketingets e-mail af 26. juni 2014 vedrørende høring om beretning 3 og dialogmødet i Folketinget den 26. august 2014, skal Forbrugerrådet Tænk hermed fremkomme med sine bemærkninger til Kulturudvalget og Retsudvalget.

Indledningsvis vil vi gerne rose udvalgene for at have sat fokus på emnet. Vi er enige i, at der er et presserende behov for at sikre de danske forbrugere en bedre beskyttelse af deres personlige oplysninger i et digitaliseret samfund og vi støtter de problematikker, som udvalgene er blevet enige om at prioritere.

Generelle bemærkninger

Overordnet set vil et højere it-sikkerhedsniveau og en styrkelse af retten til et digitalt privatliv kræve et kursskifte herhjemme – både politisk, i offentligt og privat virksomhedsregi og i forhold til forbrugerne.

For det første er der behov for, at regeringen vægter hensynet til retten til privatliv endnu højere under udviklingen af det digitale samfund. Dette gælder både indenfor digitalisering af den offentlige administration, ved etablering og centralisering af registre eller indførelse af systemkontrolfunktioner. Sådanne tiltag øger risikoen for store data-læk som i Nets/Se&Hør sagen, ligesom det netop fremsatte forslag om Arbejdstilsynets adgang til knap 3 millioner borgeres løn-oplysninger af hensyn til risikoen for social dumpning er et initiativ, der kan undergrave nærværende udvalgsarbejde.

For det andet er der behov for, at it-sikkerhed og databeskyttelse bliver et centralt anliggende og ansvar for direktionen i både offentlige og private virksomheder og ikke blot for it-chefen alene. Foruden en general opdatering af persondataloven gennem nye EU-regler, er der desuden et specifikt behov for klare regler for indsamling og anvendelse af Big data.

For det tredje er der behov for, at samspillet imellem persondatalovens juridiske beskyttelsesregler og brugen af tekniske sikkerhedsløsninger integreres, så det bliver naturligt at øge beskyttelsen gennem moderne teknologi. Samtidig er der behov for rådgivning til både private og offentlige virksomheder om brugen af privatlivs-fremmende teknologier.

For det fjerde er der behov for at styrke forbrugeren gennem øget viden og kompetencer indenfor it-sikkerhed og databeskyttelse.

Konkrete bemærkninger - 5 løsningsforslag til de aktuelle problemstillinger

1. Støt EU's nye databeskyttelsesforordning og sørg for sikre rammer indtil vedtagelse
   Som Forbrugerrådet Tænk tidligere har fremført på linje med bl.a. DI, støtter vi EU's persondataforordning, som indeholder mere detaljerede sikkerhedsregler og øger forbrugerens kontrol over egne oplysninger. Den nuværende knap 20 år gamle persondatalov er ikke længere tidssvarende. Det er derfor afgørende, at der kommer et klart mandat fra den danske regering, hvis forordningen skal vedtages i Rådet. I den mellemliggende periode bør de strukturelle rammer for øget digital sikkerhed sikres ved at stille lovmæssige krav i tråd med forordningen til både det offentlige og privates brug af privatlivsfremmede teknologier – se nærmere under 3.

2. Styrk tilsynsområdet og rådgivning af den offentlige og private sektor
   Forbrugerrådet Tænk savner et stærkt og proaktivt tilsyn, som har fokus på forbrugerbeskyttelse. Dette bør ske ved at tilsynet lægger vægt på at integrere persondataregler (jura) med private og offentlige virksomheders brug af privatlivsfremmende it-løsninger (teknologi).
   Datatilsynets tilgang til databeskyttelse er i dag stringent juridisk. En eventuel ekstrabevilling til et stærkere tilsyn bør derfor betinges af en forudgående analyse af organiseringen og uafhængigheden, større fokus på forbrugerbeskyttelse, integration af persondataregler og brug af privatlivsfremmende teknologier samt rådgivning til offentlige og private virksomheder.

   En måde at styrke et tilsyn på er desuden at indføre en pligt for virksomheder til at anmelde databrud. Det kan både få en præventiv effektivt, øge sikkerheden hos de enkelte virksomheder og lette tilsynsarbejdet.
   Endelig skal vi foreslå, at tilsynets sanktionsmuligheder øges betragteligt, da det nuværende bødeniveau ikke har en tilstrækkelig effekt.

3. Implementér erfaringer med anonymisering af data
   Brug af privatlivsfremmende teknologier kan mindske datamisbrug, fordi data ved hjælp af kryptering anonymiseres eller pseudonymiseres for uvedkommende. Det kræver imidlertid et opgør med den nuværende tendens, hvor flest mulige identificerbare data er tilgængelige for flest mulige personer - fx på sundhedsområdet. Med privatlivsfremmende teknologier, kan man fx erstatte den brede adgang til alle data med rollebaseret adgang til relevant data.

   Vi foreslår, at regeringen gør det obligatorisk for offentlige og private virksomheder at foretage privatlivskonsekvensanalyser og indarbejde privatlivsfremmende teknologier i it-løsninger – både i nuværende it-løsninger som for eksempel NemID og i kommende digitaliseringsprojekter. Værktøjerne ligger der allerede, idet Digitaliseringsstyrelsen i samarbejde med Datatilsynet har udviklet en såkaldt PIA-håndbog (Privacy Impact Assessment) til netop dette formål. Ligeledes indeholder ISO27001 en risikovurdering og det er nu op til regeringen at sikre dens udbredelse.

   Endelig vil vi anbefale, at regeringen indhenter erfaring med dansk og udenlandsk brug af privatlivsfremmende teknologier med henblik på at sikre øget fokus og udbredelse i Danmark.

4. Stil krav til private aktørers brug af personoplysninger bl.a. via sociale medier
   Den nuværende kommercialisering og udnyttelse af Big data sker i dag i et hidtil uset omfang på nettet. Det er imidlertid uklart for de fleste, hvilke oplysninger der præcis indsamles, hvad de bliver brugt til nu og på sigt herunder eventuelt

videresalg. Det drejer sig både om oplysninger, vi selv afgiver, men også om de oplysninger, der indsamles via tracking-teknologier på tværs af nettet.

Brugen af Big data er ikke klart reguleret i persondataloven, hvilket skaber usikkerhed blandt virksomheder, begrænser den positive udnyttelse af data og øger risikoen for misbrug. Forbrugerrådet Tænk anbefaler, at der fastsættes regler om brugen af Big data fx i forbindelse med en revision af den såkaldte cookie-lovgivning, som dels kan skabe gennemsigtighed på området og dels kan sikre en rimelig balance mellem virksomhedernes kommercielle interesse og forbrugerens ret til privatliv.

5. Giv forbrugernes styrke og kompetencer
Forbrugerrådet Tænk mener, at der er et presserende behov for at styrke forbrugernes viden og kompetencer og yde hjælp, så den enkelte forbruger - i det omfang det er muligt - selv kan værne om egne data og it-sikkerhed og takle udfordringerne i det digitale liv. Forbrugerrådet Tænk skal derfor opfordre til, at der gennem en finanslovsbevilling sikres tilstrækkelig og uvildig information, rådgivning og støtte til forbrugerne samt til uddannelse af børn og unge.

Såfremt I har spørgsmål til ovenstående, er I velkommen til at kontakte Forbrugerrådet Tænk for en uddybning af vores anbefalinger.

Med venlig hilsen

Formand Anja Philip
Forbrugerrådet Tænk

Seniorjurist Anette Høyrup
Forbrugerrådet Tænk

5 løsningsforslag til de aktuelle problemstillinger fra Forbrugerrådet Tænk

1. Støt EU's kommende databeskyttelsesforordning og sørg for sikre rammer indtil vedtagelse
   Klart mandat og støtte fra regeringen til EU's databeskyttelsesforordning KOM(2012)0011.
   Lovmæssige krav til offentlige og private virksomheder om at foretage privatlivskonsekvensanalyser og indarbejde privatlivsfremmende teknologier i it-løsninger med udgangspunkt i den kommende forordning.

2. Styrk tilsyn og rådgivning af den offentlige og private sektor
   Der mangler et stærkt og proaktivt tilsyn med fokus på forbrugerbeskyttelse. Et tilsyn der lægger vægt på at integrere persondataregler (jura) med brug af privatlivsfremmende it-løsninger (teknologi), og som kan rådgive private – og offentlige virksomheder herom.
   Obligatorisk pligt til anmeldelse af databrud
   Øgede sanktionsmuligheder.

3. Implementér anonymisering af data
   Obligatoriske privatlivskonsekvensanalyser og indarbejdelse af privatlivsfremmende it-løsninger i eksisterende og kommende offentlige og private digitaliserings projekter. Sikre udbredelse af konsekvensanalyser (Privacy Impact Assessment) og it-sikkerhedsstandarden ISO27001 med fx kryptering og rollebaseret adgang til relevant data. Forankring heraf på direktionsniveau.
   Indhentning af erfaringer i ind- og udland med brug af privatlivsfremmende teknologier til at sikre fokus og anvendelse i Danmark.

4. Krav til private aktørers brug af personoplysninger bl.a. via sociale medier
   Fastsættelse af regler for brug af Big data både i offentlig og privat regi. Dette kan fx ske i forbindelse med en revision af den såkaldte cookie-lovgivning.

5. Giv forbrugerne styrke og kompetencer
   Fastsættelse af en finanslovbevilling til at styrke forbrugerne og sikre uvildig information og rådgivning til forbrugere samt undervisning af børn og unge.

Birgitte Toft
Udvalgssekretariat
Christiansborg
1240 København K

København, den 28. august 2014

Høring om datasikkerhed

Jeg skal hermed på vegne af Hi3G Denmark ApS (i det følgende "3") komme med 3's bemærkninger til høring over beretning nr. 3 afgivet af Folketingets Kulturudvalg og Retsudvalg 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.

3 tager beskyttelsen af personoplysninger meget alvorligt og har bl.a. dedikeret en information security manager til det løbende arbejde med at sikre og overvåge, at data håndteres i overensstemmelse med gældende lovgivning.

3 støtter også afdækningen af, om der i dag findes sikkerhedsproblemer i relation til håndteringen af personfølsomme oplysninger, som ikke er reguleret tilstrækkeligt i gældende lovgivning.

Efter 3's opfattelse må der dog udvises forsigtighed i forhold til at drage konklusioner baseret på sager, hvor der tilsyneladende er begået decideret kriminelle forhold.

I forhold til de sager, der har givet anledning til denne høring, herunder især Se og Hør sagen, er det således efter 3's opfattelse vigtigt at få klarlagt, om det er mangler i de eksisterende lovgivningsmæssige krav til datasikkerhed, der har ført til sagen, eller om der alene er tale om overtrædelse af allerede gældende lovgivning.

I forhold til overvejelser omkring yderligere tiltag i forhold til håndteringen af persondata og tilsynet hermed bør beslutninger herom efter 3's opfattelse afvente resultatet af forhandlingerne om de nye persondataregler på EU-plan. Det vil således være naturligt i forbindelse med implementeringen af den kommende EU-regulering at overveje, om denne regulering allerede tager højde for de konklusioner, som de nedsatte udvalg når frem til, og herefter i hvilket omfang det eventuelt vil være muligt og hensigtsmæssigt at indføre danske særregler på området i tillæg til EU-reglerne.

Med venlig hilsen

Ann-Louise Hansen
Advokat

Fremtidens netværk

Big data – privacy og vækst

Man siger, at vi med internettet lever i en global landsby, hvor alle ved alt om alle – men forskellen er en langt højere grad af ulighed i adgangen til oplysningerne. Alle ved ***ikke*** alt om alle. Nogle få ved til gengæld rigtig, rigtig meget om rigtig mange.

Den ulige adgang til data

Staten, kommunerne og rigtig mange virksomheder opbevarer data. Data om dig og mig og os alle sammen og det er rigtig mange data. Det har vi ikke altid givet lov til. Vi har ikke bevidst og aktivt givet de data fra os. Og har vi for eksempel været ved lægen eller indlagt på hospitalet, har det været en nødvendighed uden alternativer. Det er uafklaret, rent juridisk, hvem der ejer disse data. P.t. opfører staten sig som om den ejer de data, der samles ind gennem den offentlige sektor og virksomhederne samler data og holder på dem. Det kan være dine indkøb, el-forbrug, dine kondital og løbetider eller hvor du er og har været henne i de sidste par uger. EU kommissionen anslår, at værdien af europæernes persondata har en potentiel vækstmulighed på tæt på 1 mia. euro frem til 2020.[1] Set fra virksomhedernes side gradueres data på deres værdi. Datamængder som kunne være til gavn for samfundet via forskning eller udvikling af programmer eller nye apps, bliver således ikke frit tilgængelige, så længe de har en værdi for virksomheden. Virksomhederne er her for at tjene penge. Et nyere men efterhånden godt brugt ordsprog hedder ”Når produktet er gratis – er det dig, der er varen”. Spørgsmålet er, hvornår vi som dataudbydere begynder at tage penge for at være produktet? Og kender vi overhovedet vores markedsværdi?

Hvad Danmark ved om dig

En mulighed er at kræve at offentlige virksomheder viser alt den data de har til rådighed om en, når man går ind på deres hjemmeside. Det kunne gøres ved en knap på alle hjemmesider, der giver adgang til at se al info de har om dig. Formålet er, at man skal kunne se mængden af data, der findes og man skal kunne se sine egne data. Princippet er, at data skal være tilgængelige for den, der har leveret dem.

Hvorfor klarere lovgivning om databeskyttelse?

Kun 26% af de europæiske brugere af sociale netværk og 18% af brugere, der handler på nettet føler at de har fuldstændig kontrol over deres persondata på nettet.

43% af europæiske internetbrugere mener, at de er blevet spurgt om flere informationer end nødvendigt.

58% af europæiske forbrugere føler, at der ikke er et alternativ til at oplyse krævede personlige oplysninger ved køb eller service på nettet.

90% af europæerne ønsker samme lovgivning over hele Europa.

Kilde: Factsheet ”Why do we need an EU data protection reform? http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm

Privacy by default

Når man besøger private virksomheders hjemmesider bliver der opsamlet en ukendt mængde data. Ikke bare om, hvad du foretager dig lige nu på denne specifikke hjemmeside, men også via cookies om, hvad du ellers foretager dig på nettet. Løsningen på det er privacy by default. Dvs. et software design koncept, der forhindrer opsamling, fremvisning eller videregivelse af enhver form for personlige data uden eksplicit tilladelse fra brugeren. En af sidegevinsterne ved

[1] Factsheet: Data protection: Progress on EU reform now irreversible after European Parliament vote, 12. Marts 2014: http://ec.europa.eu/justice/data-protection/law/index_en.htm

privacy by default er, at mange brugere ikke ved eller kan gennemskue, hvilke og hvor mange oplysninger om dem, de videregiver ved at besøge en hjemmeside eller være aktive på de sociale medier. Udfordringen er at finde en standard, der tager højde for forskellige typer software, forskellige brugerbehov og som virker, hvor den skal. Men uden at blive et forstyrrende irritationsmoment ved for eksempel konstant at præsentere brugeren for advarsler og krav om godkendelse, før man kan komme videre.

Big data CSR

En anden mulighed er at skabe et valg for brugeren. Når vi køber dagligvarer som kaffe kan vi vælge bæredygtige mærker. Når vi køber ind på nettet kan vi vælge web-butikker med e-mærket. Det har en omkostning, ofte på prisen, alligevel er det et marked, der er vokset voldsomt de seneste 10 år. På samme måde burde man kunne vælge hjemmesider, der tager hensyn til dit behov for privacy. En privacy-venlig hjemmeside kunne give mulighed for at vælge en "valgt fra" knap. Det giver mulighed for at vælge information eller handlinger fra, hvis du synes, at du i samme omgang afgiver for mange informationer. Omvendt kan man også give mulighed for at afgive information, hvis det er en fordel. Nogle kan for eksempel se det som en kæmpe fordel, at man ved at afgive informationer via GPS om, hvor man kører, kan modtage gode råd om trafikforhold, benzinforbrug, servicestationer og kørselsøkonomi. Andre vil gerne kunne køre uden at der bliver registreret andet end for eksempel vejtype eller hvor meget man har kørt indenfor et større område.

Konkret kan det gøres ved at klassificere ved hjælp af vejledning og standardisering.

Privacy
Privacy handler ikke om at skjule oplysninger, men om retten til at kunne bestemme over informationer om os selv.

Privacy by design
Når hensyn til privatlivet tages med i opbygningen af systemet. Privacy by design er kendetegnet ved 7 fundamentale principper:
1. Det er proaktiv beskyttelse,
2. privacy by default, dvs. automatisk beskyttelse som standardindstilling,
3. privacy er indlejret i it-design og ikke noget man vælger til,
4. beskyttelse ses som plussum og ikke som et trade off med f.eks. sikkerhed,
5. fuld –livscyklus beskyttelse, hvor data bliver sikkert opbevaret og sikkert destrueret,
6. uanset hvilken praksis, der bruges skal det være åbent og verificerbart for alle og endelig
7. brugercentreret, dvs. brugervenligt og med fokus på brugerens privatliv.

Privacy by default
En standardindstilling, der forhindrer indsamling, visning eller videregivelse af personlige data.

Big Privacy
Er baseret på Privacy by design men udvidet til også at omfatte netværk, værdikæder og økosystemer ved brug og produktion af Big data.

Standarder for privacy
Der findes følgende standarder til beskyttelse af privatlivets fred på internettet:

- ISO 27001

Tidssvarende lovgivning er det nødvendige udgangspunkt

Den nuværende lov om persondatabeskyttelse er 19 år gammel, forældet og yder for svag beskyttelse. Det er afgørende vigtigt med lovgivning – virksomhederne gør det ikke af sig selv. Lovgivning kan være med til at sikre motivation for at der investeres i kryptering. Og samtidig er netop klar lovgivning en af forudsætningerne for at virksomheder tør binde an med Big data. Selv med god velvilje kan det være svært at gennemskue, hvor grænserne går, når det gælder personfølsomme oplysninger. Jura er derfor et vigtigt pejlemærke for, hvad der er i orden og hvad der ikke er acceptabelt.

Men samtidig er udfordringen: Hvad hjælper lovgivning, hvis vi ikke ved, at den er brudt? Dataopsamling sker "bagved". Der er behov for meget skarpere datarevision, så virksomhederne ikke overtræder reglerne. Man kan sammenligne med karteldannelse, hvor den største udfordring er opdage, hvad der faktisk foregår.

Big data og persondata har tre brudflader, der skal tages vare på:

Data høst: Når der opsamles data i dag er det langt fra altid, at de enkelte borgere aktivt har givet tilsagn om at deres private data må opsamles og hvad de må bruges til. Og ofte er folk slet ikke klar over, hvad der registreres.

Data mining: Her renses data og analyseres i forhold til andre data med det formål at skabe sammenhæng mellem aktuelle forhold og dermed give os ny viden. Det kan være i forskningssammenhænge, men det kan også være til rent kommercielle forhold.

Applikationsfasen: Datamining resulterer i en algoritme, der er en generaliseret form af den nye viden. Værdien af den ligger i koblingen til den virkelige verden, f.eks. et datasæt af skoleelever eller kunder. Afhængig af algoritmen kan man herved for eksempel forudsige handlinger eller præferencer. Et kendt eksempel er "Dem, der lånte denne bog, kunne også lide xxx". Mere bekymrende kan det blive, når man forsøger at differentiere priser på eksempelvis rejser alt efter, hvilke præferencer man i øvrigt ved at kunden har. Et eksempel på det er Safari-sagen.[2]

En lovgivning på området skal tage hensyn til disse tre brudflader og til at der i dag er tale om langt større muligheder for opsamling af data og samkøring af data meget hurtigt og meget billigere end tidligere.

Skadevolder betaler

Sikkerhed kan også motiveres ved at betale for omkostningerne ved fejl. Eksempelvis ved identitetstyveri, der har både store menneskelige, men også økonomiske konsekvenser for den, der rammes. Firmaer bør modsat i dag have pligt til at oplyse, når der sker datalæk og de skal bære de økonomiske omkostninger ved "oprydningen" ved f.eks. identitetstyveri. En metode er altså at kunne gøre sikringen af brugernes privatliv til et problem for de udbydere, der indsamler data.

Hvem holder øje?

Det er Datatilsynet, der fører tilsyn med om reglerne overholdes i Danmark. Men antallet af inspektioner er ikke vokset i takt med udviklingen på internettet[3]. Det er afgørende, at Datatilsynet har ressourcerne og uafhængigheden til at kunne løfte overvågningsopgaverne i takt med at digitaliseringen stiger både private og i det offentlige. Både fordi vi som privatpersoner bruger nettet mere og mere, men også som en logisk konsekvens af den stigende digitalisering af den offentlige sektor og frigørelse af offentlige data. Presset på sikkerheden stiger med digitaliseringen og det stiller krav til vogterne. Et bud kan også være at supplere med et skarpere tilsyn med reglerne ved hjælp af datarevisorer som vi kender det fra regnskabsrevisorer.

---

[2] Læs mere på conferences.sigcomm.org/co-next/2013/program/p1.pdf

[3] Se http://www.datatilsynet.dk/publikationer/datatilsynets-aarsberetninger/

EU kommissionens Data Protection Reform er vejen frem

EU kommissionens Data Protection Reform også kendt som persondataforordningen, er en vigtig milesten på vejen til en mere fair og tillidsvækkende brug af de muligheder Big data giver. EU er på dette område en vigtig frontløber. Desværre støtter Danmark ikke forordningen pga hensyn til forvaltningstraditionen, modsat de øvrige lande. En lang række interesseorganisationer, herunder DI, PROSA, Forbrugerrådet Tænk m.fl. støtter reformen. Hovedpointerne heri er bl.a.:

Retten til at blive glemt: Bedre adgang til at få ens data slettet, når man vil det.

Dataportabilitet: Herunder at flytte egne oplysninger fra én udbyder til en anden.

Kontrol over egne data: Retten til aktivt at sige ja til opsamling af persondata og virksomheders og organisationers pligt til at advare ved brud på datasikkerhed.

Databeskyttelse først: Privacy by design og Privacy by default indgår som krav i EU's personadataforordning, også ved f.eks. sociale netværk.

FN's Verdenserklæring om Menneskerettigheder 1948, artikel 12:
"No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks".

Den Europæiske Menneskerettighedskonvention, 1950, artikel 8, stk.1:
"Enhver har ret til respekt for sit privatliv og familieliv, sit hjem og sin korrespondance".

Uddannelse og dannelse

Big data åbner en verden af nye muligheder. Det stiller krav og modkrav. Hvordan får vi mest muligt ud af de nye muligheder og hvordan lærer vi at begå os i en verden, der ikke glemmer. Beskyttelse af privatlivets fred og sikring af it-sikkerhed i det hele taget, kræver en indsats på flere fronter. Både når det gælder uddannelsen af de it-specialister, der udvikler systemerne, og når det handler om at lære folkeskolebørnene at gebærde sig i det digitale samfund.

Uddannelse af ingeniører og teknikere

Erhvervsstyrelsen har i deres analyser konstateret en tendens til stigende efterspørgsel efter analytikere med stor indsigt i håndtering, strukturering, analyse og visualisering af data. Kernegruppen af eftertragtede analytikere består af matematikere, statistikere, dataloger, ingeniører og økonomer med de rette kompetencer.[4] Danmark er i front på områder som befolkningens IT-parathed, men udviklingen går langsomt, når det gælder Big data. Der er derfor behov for en målrettet indsats i forhold til at styrke uddannelserne og efteruddannelserne på netop de kompetencer der kræves ved håndtering af Big data, hvis ikke vi skal falde helt bagud.

Samtidig er det vigtigt, at uddannelse og efteruddannelserne også får mere fokus på risici ved IT-sikkerhed og brud på privacy. Teknologi er hverken mere eller mindre end det, den bliver brugt til. Men i takt med at teknologien kan mere og mere, bliver risikoen for misbrug og konsekvenserne ved fejl som f.eks. lækager langt større. Skal vi bevare tilliden til fordelene ved Big data, skal bevidstheden om, hvordan IT-professionelle bruger data skærpes.

[4] "Big data som vækstfaktor i dansk erhvervsliv", Erhvervsstyrelsen, Irisgroup, december 2013.

Big data kan skabe

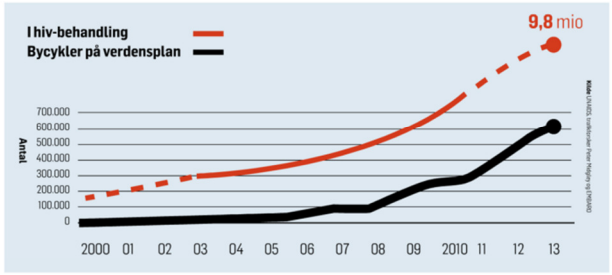
- Ny viden
- Optimering af ressourcer
- Forudsigelser
- Overvågning

Om resultatet bliver til noget positivt eller negativt afgøres af måden vi bruger data på.

Human sensors og naturkatastrofer

Blandt de mere dramatiske, men også mest avancerede eksempler på brug af Big data er et forskningsprojekt på University of Illinois, USA, hvor professor Tarek Abdelzaher har fokus på social sensing og hvordan man får pålidelige informationer ud af "upålidelige" data som eksempelvis tweets under begivenheder som orkaner, jordskælv eller civile uroligheder. Kan man opsamle informationer fra menneskelige sensorer kan det være et afgørende parameter for at klarlægge omfanget af en katastrofe og sende den rigtige hjælp ud allerede mens det står på. Her er det ikke selve høstningen af data, der er problemet, da tweets netop er helt åbne og offentligt tilgængelige informationer givet bevidst af brugeren. Brugt på den rigtige måde kan det til gengæld effektivisere livsvigtigt rednings- og hjælpearbejde.

Skal forudsigelser have konsekvenser, så er det afgørende at være på det rene med, at statistisk signifikant sammenhæng ikke nødvendigvis er det samme som en videnskabeligt bevist sammenhæng. Korrelation medfører ikke kausalitet. Udfordringen blandt de kommende IT-professionelle er at sikre en bevidsthed omkring, hvordan vi sikrer at brug af data ikke ender i brud på sikkerheden eller ulovlig overvågning. Ligesom man skal være opmærksom på, om de nye sammenhænge som Big data afdækker, faktisk er sande, så vi ikke risikerer falske forudsigelser:



Datajournalistik: Bycykler sikrer hiv-behandling

Skal vi sikre privatlivets fred skal privacy tænkes ind i og i langt højere grad integreres i vores software, som det eksempelvis gøre i privacy by design-tankegangen – det skal ingeniørerne opdrages til.

"Hvis det er gratis, er det dig, der er varen"

Brugerne skal opdrages til, at der ikke er noget, der hedder gratis. Virksomhedernes forretningsmodel er, at de ganske vist giver dig gratis adgang til at bruge f.eks. et spil, en app eller et socialt medie. Til gengæld får de masser af forbrugerdata tilbage, som de kan bruge til markedsføring, videresalg mv.

Hvis man kan gøre forbrugerne mere bevidste vil det også ændre virksomhedernes fokus, så tilbud om øget privacy bliver et konkurrenceparameter.

Bekymringen i befolkningen er stigende, men holdningen til, hvor grænserne går, er vidt forskellige. Der er endnu ikke en fasttømret kultur for, hvad der er acceptabelt og hvor vi sætter grænserne. Der er omvendt heller ikke endnu en bred erfaring med, hvad der er konsekvenserne af at udlevere oplysninger, ligesom det langt fra altid er klart for folk, hvor mange oplysninger man afgiver, eksempelvis ved at downloade en app som spillet "Angry birds".

Samtidig er forholdet til, hvad der er en del af privatlivet forskelligt i forskellige lande. I Sverige og Norge er alle selvangivelser eksempelvis offentlige. I England er kameraovervågning i det offentlige rum acceptabelt i langt højere grad end

i Danmark, til gengæld er der en lettere forbløffet skepsis overfor vores CPR-nr. system. Et projekt om road pricing i Nordjylland viste, at nogle af bilisterne ser en klar fordel i at kunne overvåge børnene, når de låner bilen. Og man kunne nemt forestille sig, at nogle gerne bytte private data for bilkørsel for mere og bedre information om kørsel i egen bil.

Men konsekvenserne er begyndt at vise sig og det har en effekt. På EU niveau siger 70 % af de adspurgte europæere, at de er bekymrede. Flere lækager og en stigning på 77 % i datakriminalitet betyder, at der nu er en tendens til at det begynder at vende i befolkningernes holdninger.

Konklusion: Forebyggelse er billigere end…

Der er store fordele ved brug af Big data i forskning og i den offentlige sektor. Der er også meget, der tyder på, at der er en erhvervsfordel for Danmark ved at lade virksomheder få et eller andet niveau af adgang til de mange oplysninger om danskernes helbred, læge- og medicinforbrug lagret i cpr-registret i gennem snart en generation. Men en forudsætning for at vi kan dette er tillid til, at vi ikke pludselig står overfor negative konsekvenser i form af dyrere priser på eksempelvis rejser eller forsikringer, identitetstyveri eller offentliggørelse af følsomme oplysninger, for eksempel om vores helbred.

En måde at sikre fordelene og undgå ulemperne er at integrere data efter principperne i Privacy by Design. En anden er at skabe et etisk kodeks for, hvad der er god praksis for virksomheder på nettet. En tredje er at skabe efterspørgsel efter privacy niveauer, altså, at man som bruger kan vælge det niveau af åbenhed man er klar til. Formålet er ganske enkelt, at man som bruger er bevidst om, at man er en del af en handel og derfor selvfølgelig bør forhandle sig til den bedst mulige pris. Men også, at man giver rum for, at folk, der er villige til at afgive oplysninger også kan få fordelene af eksempelvis bedre trafikinformation eller mere målrettede reklamer.

Et dansk etisk moralkodeks?

Den engelske Information Commissioner's Office (ICO) har publiceret "Anonymisation: managing data protection risk", november 2012. Denne code handler om risikohåndtering i forbindelse med personfølsomme data og er et led i den britiske "open data agenda".
Se mere på:
http://search.ico.org.uk/ico/search?q=anonymisation%3A+managing+data

I Danmark har Datatilsynet en række vejledninger på deres hjemmeside, se www.datatilsynet.dk

IDA anbefaler

- Private og offentlige virksomheder bør på en let tilgængelig måde oprette adgang til alle de oplysninger som den pågældende virksomhed har om dig og hvad der ikke bliver slettet, når du forlader siden, f.eks. ved at man kan trykke på et ikon/knap.
- Privacy bør være en standardindstilling og ikke noget man skal gøre aktivt for at sikre. Der bør i højere grad udvikles pc'ere med indbygget software så fx browsere allerede har default indstillinger med højt privacy niveau, ligesom man allerede nu kan købe tablets med børnesikkerhedsindstillinger
- Kommunikation med det offentlige skal krypteres efter principperne om anbefalet post.
- Uddannelserne skal have fokus på privacy, sikkerhed og databeskyttelse.
- Etik og moral-parametre baseret på konsekvensrisiko skal fremmes på uddannelserne, så de unge kan sige fra, når kommende arbejdsgivere kræver uetiske ting af dem.
- IDA støtter den nye EU forordning på niveau med DI, PROSA og Forbrugerrådet Tænk, Institut for Menneskerettigheder m.fl.
- Forureneren betaler-princippet bør indføres. Omkostninger ved IT brud på sikkerheden og identitetstyveri betales af udbyder, fx bank eller virksomhed.
- Nødvendigt, at der sker en opdatering af lovgivningen, så den modsvarer det teknologiske kvantespring som Big data giver.
- Datatilsynet styrkes til at kunne rådgive om Big data, udstikke retningslinjer på niveau med ombudsmanden og gøres uafhængigt.
- Der skal startes pilotprojekter op med øget rådgivning til virksomheder om krav til privacy og mulighederne for at markedsføre sig på god skik.

- Det bør overvejes om der er behov for at supplere med krav om IT-revision.
- IDA bør udvikle et etisk kodeks som medlemmer skal overholde.

Vil du vide mere?

Kontakt
Chefkonsulent Grit Munk
gmu@ida.dk, tlf: 30596596

Chef for Politik, Presse og Analyse Søren Lauridsen,
sla@ida.dk, tlf: 30637723

Gør verden til et bedre sted med Big data

De nye muligheder for samkøring af data giver kæmpe fordele. Brugt på den rigtige måde er der både erhvervsmæssige, personlige og stor samfundsmæssige gevinster at hente. Men er vi gearet til at udnytte mulighederne bedst muligt?

Hvad er Big data og hvad kan vi med det?

Begrebet Big data er relativt nyt – til gengæld bruges det rigtig tit. Men det er en usikker størrelse med løbende nye bud på definitioner. Den klassiske definition er store mængder af meget forskellige data fra forskellige kilder, behandlet i højt tempo. Store mængder af data skal i denne sammenhæng forstås som et så stort antal informationer, at traditionelle måder at behandle data på ikke er nok. Men Big Data er ikke blot mange data, det er også data fra mange forskellige kilder og dermed bliver pålidelighed i data en vigtig faktor.

Big data har et åbenlyst potentiale især ved bedre brug af ikke-personfølsomme data. Det skal udnyttes. Men Big data hænger ofte uløseligt sammen med persondata. Det er fra datamining af persondata, at de store økonomiske værdier ligger. Hvor Big data ofte betegnes som det nye sort, så er persondata betegnet som "the new oil". Og hvis persondata er ny olie, så er Big data den "maskine", der skal pumpe det op.[1] Omvendt, hvis vi ikke tager hensyn til privatlivets fred og persondatasikkerheden, så forsvinder tilliden til at lade persondata indsamle og dermed tørrer oliekilden ud.

EU kommissionen anslår, at værdien af europæernes persondata har en potentiel vækstmulighed på tæt på 1 mia. euro frem til 2020.[2] Hvis Big data skal være en kilde til vækst i Danmark, skal vi blive bedre til at bruge denne "maskine", så vi får mest muligt ud af den, men vi skal i høj grad også gøre den nye olie til en vedvarende energikilde. Det gør vi ved at sikre de følsomme persondata mod lækager, misbrug og offentliggørelse. Indsatsen vil skulle gå på tre ben: Strammere og mere klar lovgivning, CSR og mulighed for mere bevidst personlig adfærd.

Definitioner af Big data:

Gartner's klassiske 3 V'er:
Big data er kendetegnet ved:
Volume (mængde): Større mængder af data end normale systemer kan håndtere.
Velocity (hastighed): Højt tempo i datatilstrømning.
Variety (mangfoldighed): Mange forskellige datatyper og kilder.
Efterfølgende er endnu et v blevet foreslået:
Veracity: Sandfærdighed eller måske mere korrekt, pålidelighed. Hvordan kan vi sortere mellem pålideligheden af de mange data.

Hvor stort er store mængder data?
En anden definition giver en vigtig indikation af dette:
""Big data " refers to datasets whose size is beyond the ability of typical database software tools to capture, store, manage, and analyze".

Big data technologies:
En ny generation af teknologier og arkitekturer, designet til økonomisk at udtrække værdi fra meget store mængder data, ved i højt tempo at opsamle, opdage og eller analysere data.

Kilde: Wikipedia, 29.01.2014 og Ann Covoukian & Jeff Jonas.

[1] Big Privacy: Bridging Big data and the Personal Data Ecosystem Through Privacy by Design, Ann Cavoukia & Drummond Reed

[2] Factsheet: Data protection: Progress on EU reform now irreversible after European Parliament vote, 12. Marts 2014: http://ec.europa.eu/justice/data-protection/law/index_en.htm

Ingeniørforeningen, IDA
Kalvebod Brygge 31-33
DK-1780 København V
+45 33 18 48 48
ida@ida.dk
ida.dk

Big data som game changer

Springet fra tidligere registrering af data til Big data handler om mængder som er langt større end tidligere. Men den afgørende forskel er at data indsamles fra en langt større mængde og variation af kilder. Eksempelvis begynder virksomheder ikke bare at trække på egne data, men også på data fra kunder og leverandører, sensorer i de produkter virksomheder har solgt, offentlige registre og datasamlinger, sociale medier etc. Disse forskellige data indsamles og behandles med nye typer algoritmer og bedre computerregnekraft og kan være med til at styrke virksomhedens beslutningsgrundlag. Dette giver mulighed for ikke bare at lave en evaluering af, om det man har gjort er godt nok, men også fremadrettet at forudsige, hvor virksomheden skal sætte ind i forhold til at skaffe flere og bedre kunder eller f.eks. undgå slidtage og fejlmeldinger på produkter.

Det er endnu få danske virksomheder, der for alvor udnytter mulighederne og udviklingen går lidt langsommere end i andre lande. For dem, har der ofte været tale om en gradvis udvikling, hvor de over tid har investeret i bedre registrering og ajourføring af egne data, inddragelse af nye eksterne datakilder, bedre software og værktøjer og dygtigere analytikere. Blandt SMV'erne er det kendetegnet, at de enten har en lang tradition for indsamling af data eller er meget ingeniørtunge.

Blandt de afgørende forudsætninger for at kunne bruge Big data er:

1. Højt videns- og kompetenceniveau indenfor data, teknologi og dataanalyse
2. Høj grad af digitalisering i virksomheden
3. Der er ofte et spring til nye forretningsmodeller, f.eks. hvor service og rådgivning knyttes direkte til produktet.

Blandt barriererne er omvendt stigende mangel på analytikere, manglende adgang til offentlige data, uklare regler for anvendelse af personfølsomme data og hjælp i form af rådgiving og støtte til at komme i gang. [3]

Eksempler på brug af Big data i danske virksomheder

Overblik over egne data:
Grundfos har opbygget et Enterprise Ressource Productivity (ERP) system, hvor virksomheden blandt andet lagrer alle interne transaktionsdata, produktionsdata, logistikdata, mv. i alt ca. 5 petabytes data (5 millioner gigabytes). Systemet er brugt ved analyser, der har ført til effektiviseringer i produktionen og i arbejdsgangene.

Kombination af egne og andres data:
Saxo.com har brugt sine egne salgssdata om bøger i kombination med eksterne demografiske data til at udvikle en anbefalingsalgoritme, der bruges til at anbefale endnu en bog, når den første er lagt i "indkøbskurven". Det betød en stigning i salget på 12 %.

Datadreven innovation:
Hapti.com udvikler online spilprodukter og bruger data-aftryk fra kundernes brug af spilprodukter til løbende produktudvikling ud fra kendskab til frafaldsmønstret for forskellige aldersgrupper, der kan indikere om spil er for svære eller for kedelige.

Optimering af kundeservice:
Vestas anvender Big data til at forkorte beregningsperioden og til at give et bedre statistisk beslutningsgrundlag for opstilling af vindmøller, bl.a. fordi måleperioden kan forkortes fra 18 måneder til 15 minutter. Vestas udviklede i 2010-2011 "Firestone Computer" sammen med IBM, den største og hurtigste computer i Danmark og i 2011 den 3. største kommercielle computer i verden.

Kilde: "Big data som vækstfaktor i dansk erhvervsliv", Erhvervsstyrelsen, Irisgroup, december 2013.

[3] "Big data som vækstfaktor i dansk erhvervsliv", Erhvervsstyrelsen, Irisgroup, december 2013.

Business case eller samfundsinvestering

Infrastruktur og forskning i sundhed er blandt de områder, hvor Big data kan være en game changer.

Brug af det danske CPR-register og EPJ er et positivt eksempel på offentlig anvendelse af Big Data i forbindelse med for eksempel kræftforskning og sundhedsanalyser. Et andet eksempel er sporing af fordærvet kød, der via bon'er kan spores til konkrete købere.

Transportdata kan bruges til at optimere folks kørsel/transportvaner vel at mærke uden at man derved kompromitterer privacy. Det gøres eksempelvis af Transport for London, TfL. TfL opsamler data og lægger ud, hvem uden at man kan se, hvem der er afgiver af data.

Den 1. januar 2013 blev der givet fri adgang til en række offentlige grunddata. Dette har allerede givet grundlag for en række virksomheder.[4]

En samfundsmæssig gevinst kræver, at vi sikrer, at vi får mest muligt ud af de data, der indsamles. Der er imidlertid to udfordringer, der skal løses før det kan lade sig gøre.

For det første er det en udfordring, hvis det offentlige tjener penge på at holde på de data, der er opsamlet. Det gælder især, hvis det ligefrem ligger i forretningsplanen, at der skal tjenes penge på brug af data. Digitaliseringsstyrelsen er i gang med at få det offentlige i spil. Men ikke i alle tilfælde er der en businesscase. Her bør det overvejes om ikke der er samfundsgevinst i at infrastrukturejerne, f.eks. staten og kommunerne, investerer i f. eks. trafikdata, som en investering i effektiv udnyttelse af vejnettet.

Men også virksomhederne er nærige med informationer. De mest nyttige informationer til brug for viden om god kørsel er f.eks. låst i bilerne fra producenternes side. Så selv om man måske nok kunne forestille sig, at en del bilister gerne bytte private data for bilkørsel for mere og bedre information om kørsel i egen bil, så er det ikke muligt at lave det optimale sammenligningsværktøj.

Det ultimative krav er selvfølgelig, at hvis ikke-personfølsomme data er opsamlet, så skal de udleveres til den data vedrører, f.eks. ejeren/føreren af bilen. Et minimums krav må være, at der i langt højere grad bliver låst op for adgang til ikke-personfølsomme data, som minimum der, hvor der er tale om det offentlige Danmarks data. For virksomhederne bør der oprettes et samlingspunkt, en portal, hvor virksomheder kan udbyde og byde på datamængder. Den anden udfodring er, at loven bliver klar at følge for virksomhederne og vækker den nødvendige tillid blandt befolkningen.

Usikkerhed om lovgivning er en barriere

EU kommissionens Data Protection reform er en vigtig milesten på vejen til en mere fair og tillidsvækkende brug af de muligheder Big data giver. Hovedpointerne heri er bl.a.

Ét kontinent – én lov: En samlet lov vil give større sikkerhed og klare linjer for både brugere og virksomheder og mindre bureaukrati for virksomhederne, da man ikke længere skal forholde sig til 27 forskellige sæt dataregler.

One-stop-shop: Virksomheder vil herefter kun skulle forholde sig til én myndighed.

Samme regler og mindre bureaukrati: Ens vilkår for alle virksomheder, der opererer i EU-landene, uanset om de er placeret i eller udenfor EU.

En samordning af regler og praksis forventes at kunne spare europæiske virksomheder for 2,3 mia. euro om året. Samtidig forventes det, at stærkere og klarere regler vil opbygge tillid til europæiske virksomheder, hvilket vil være en global konkurrencefordel efterhånden som netop privacy vil få større og større opmærksomhed.

[4] "Big data som vækstfaktor i dansk erhvervsliv", Erhvervsstyrelsen, Irisgroup, december 2013.

IDA anbefaler

- At regeringen udarbejder en handlingsplan for, hvor Big data kan være med til at forbedre velfærden i Danmark, herunder, hvordan man styrker virksomhedernes kendskab til og brug af Big data.
- At stat, regioner og kommuner stiller ikke-personfølsomme data til rådighed og fri afbenyttelse
- At de ikke-personfølsomme offentlige data lægges frem, i en let tilgængelig form fra samme portal, ligesom der med fordel kunne oprettes en portal for private virksomheders køb og salg af ikke-personfølsomme data.
- At regeringen udvikler en strategi for, hvordan man støtter op om brugen af design af personfølsomme data efter principperne i privacy-by-design, så de bliver brugbare i anonym form og ikke ved hjælp af samkøring med andre data kan de-anonymiseres, dvs. at man kan identificere individer bag de personfølsomme oplysninger. Dette kunne konkret gøres ved markedsføring af gode eksempler.
- At der skabes de nødvendige forsknings- og uddannelsesmæssige miljøer i Danmark på verdensniveau, der kan sikre fremtidige kompetencer hos matematikere, dataloger, ingeniører m.v. i forhold til at arbejde med big data analyseværktøjer, store datamængder, varierende kilder som tekstdata og data fra f.eks. human sensors, samt den nødvendige forståelse for de sikkerhedsmæssige perspektiver.

- At der skabes efteruddannelsesmiljøer, der kan styrke kompetencerne hos matematikere, dataloger, ingeniører m.v. i forhold til at arbejde med big data analyseværktøjer, store datamængder, varierende kilder som tekstdata og data fra human sensors, samt den nødvendige forståelse for de sikkerhedsmæssige perspektiver

Vil du vide mere?

Kontakt
Chefkonsulent Grit Munk
gmu@ida.dk, tlf: 30596596

Chef for Politik, Presse og Analyse Søren Lauridsen,
sla@ida.dk, tlf: 30637723

Ingeniørforeningen, IDA

Kalvebod Brygge 31-33
DK-1780 København V
+45 33 18 48 48

ida@ida.dk
ida.dk

Ingeniørforeningen, IDA
Kalvebod Brygge 31-33
DK-1780 København V
+45 33 18 48 48

ida@ida.dk
ida.dk

Retsudvalget
Att: Birgitte Toft-Petersen
Birgitte.toft-petersen@ft.dk

Svar på Høring over beretning nr. 3 afgivet af Folketingets Kulturudvalg og Retsudvalg

29. august 2014

Ingeniørforeningen, IDA tillader sig hermed at afgive høringssvar på udsendte beretning nr. 3 afgivet af Folketingets Kulturudvalg og Retsudvalg.

Først og fremmest vil vi rose de to udvalg for at nedsætte 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. Begge dele er hårdt tiltrængt.

Vi vil gerne rose udvalgene for at bede regeringen om at udvide det tværministerielle udvalgs fokus områder til at omfatte alle områder, hvor der opbevares personfølsomme oplysninger og data. Det er Ingeniørforeningen, IDAs vurdering, at der er enorme fordele ved at styrke digitaliseringen af Danmark, både samfundsmæssige og for den enkelte borger.

Det gælder den offentlige sektor, der vil kunne tilbyde bedre service til både borgere og virksomheder. Det gælder uddannelse og forskning. Det gælder virksomheder, der med digitalisering kan blive mere effektive, blive stærkere på innovation og eksportnetværk og til at inddrage Big data. Big data vil være en af de store fremtidige kilder til produktudvikling gennem indsamling og brug af data fra varierende kilder, men stiller samtidig øgede krav til sikkerhed og etik omkring brug af data.

Men det gælder også den almindelig dansker, der vil kunne kommunikere effektivt med det offentlige, blive bredere og hurtigere informeret, få bedre og mere varierede muligheder i forbindelse med skole og uddannelse og endelig nyde godt af sociale medier, streaming og spil mm.

Hvis alle disse fordele skal høstes, så er det afgørende, at vi som danskere bevarer den tillid vi har til at kunne bruge internettet og de mange digitale medier og devices, dvs. mobiltelefoner, pc'er, tablets, gps'er etc. der efterhånden er blevet en fast del af vores hverdag. Man skal kunne gå trygt til lægen, deltage i forskningsprojekter, søge bøger og informationer om alt det, man har brug for at vide på nettet uden at lægge bånd på sig selv, fordi man er bekymret for, om nogen kigger

med. Det er en vigtig del af det at være borger i et demokratisk land og i en moderne veldrevet velfærdsstat.

Vi tillader os at vedlægge to korte papirer, der skitserer Ingeniørforeningens holdninger til IT sikkerhed og Big data i håbet om, at det kan inspirere arbejdsgruppens arbejde. Papirerne er udarbejdet i et samarbejde med bl.a. DTU Compute, Rådet for Større Datasikkerhed og Forbrugerrådet. Holdningerne er dog vores eget ansvar.

Derudover stiller vi os selvfølgelig gerne til rådighed med ekspertise på ikke mindst den tekniske del af it sikkerhed. Ingeniørforeningen, IDA har godt 6000 IT-professionelle medlemmer, der er organiseret i IDA IT. Her står netop it-sikkerhed højt på listen.

Blandt de mange vigtige indsatsområder ser vi bl.a.:

- En opdateret persondatalov, der tager højde for ikke mindst de teknologiske muligheder som ikke var en mulighed under lovgivningens tilblivelse. Herunder bl.a. Big data og de sociale medier.

- Dansk støtte til EU's nye databeskyttelsesforordning.

- Styrkelse af Datatilsynets kompetencer og ressourcer.

- Effektiv anonymisering af datasæt til brug ved forskning og kommerciel udnytttelse.

- Krav om indførelse af privacy by design og privacy by default (se yderligere i vedlagte bilag).

- Obligatorisk vurdering af databeskyttelse for både offentlige digitaliseringsprojekter og private digitaliseringsprojekter, der omfatter samarbejde med eller brug af offentlige data.

Med venlig hilsen og ønske om god arbejdslyst,

Grit Munk
Chefkonsulent
Analyse, Politik og Presse
Ingeniørforeningen, IDA

INSTITUT FOR
MENNESKE
RETTIGHEDER

WILDERS PLADS 8K
1403 KØBENHAVN K
TELEFON 3269 8888
DIREKTE 3269 8805
RFJ@HUMANRIGHTS.DK
MENNESKERET.DK

Folketingets arbejdsgruppe
vedrørende datasikkerhed
Birgitte.Toft-Petersen@ft.dk

J. NR. 540.10/30991/RFJ/MAF

29. AUGUST 2014

HØRING OVER BERETNING NR. 3

Folketingets arbejdsgruppe om datasikkerhed har ved e-mail af 26. juni 2014 anmodet om Institut for Menneskerettigheders eventuelle bemærkninger til beretning nr. 3 afgivet af Kulturudvalget og Retsudvalget den 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.

Instituttet har følgende bemærkninger:

Institut for Menneskerettigheder hilser den parlamentariske arbejdsgruppe vedr. databeskyttelse velkommen. I takt med den stigende digitalisering er der et øget behov for at sikre et højt niveau af databeskyttelse og informationssikkerhed i Danmark. Som illustreret i beretningen dækker området over en bred række af problemstillinger, der knytter sig til såvel det retlige grundlag, det interne og eksterne tilsyn med området, områdets internationale karakter, borgerens retssikkerhed, mv.

Behovet for øget fokus på databeskyttelse har været fremhævet i instituttets årlige statusrapport i såvel 2012 som 2013. Statusrapportens kapitel om databeskyttelse omhandler blandt andet de danske logningsregler, kontrol med sociale ydelser, sociale medier, cloud computing, samt reguleringen af, og kontrollen med, politiets efterretningstjeneste. For hvert område er angivet en række anbefalinger til regeringen.

Som supplement til statusrapporten vil instituttet fremhæve følgende tre indsatsområder, som instituttet anser som væsentlige i forbindelse med arbejdsgruppens arbejde.

EN STYRKET INDSATS FOR INFORMATIONSSIKKERHED OG DATABESKYTTELSE

Databeskyttelse og informationssikkerhed behandles ofte som enten juridiske eller tekniske emner, frakoblet hinanden. Hvis informationssikkerhed og databeskyttelse skal gennemsyre praksis i institutioner og virksomheder, kræver det et tæt samspil mellem retlige standarder, organisation og teknologisk løsning. Området bør opprioriteres politisk, og det bør forankres med både teknisk, organisatorisk og juridisk kompetence for eksempel i form af et ressortministerium, en ombudsmand på området eller en offentlig institution. Danmark mangler en stærk tværfaglig instans som kan rådgive, monitorere og tilse det brede område som databeskyttelse og informationssikkerhed dækker over i både offentlige institutioner og private virksomheder.

EN SAMLET STRATEGI FOR INFORMATIONSSIKKERHED OG DATABESKYTTELSE I DEN OFFENTLIGE SEKTOR

Der er igangsat en kortlægning af sikkerheden ved betalingskort. Dette arbejde kan imidlertid ikke stå alene og der er behov for en bredere undersøgelse af, hvordan man kan forbedre sikkerheden ved behandling af personoplysninger i den offentlige sektor. Som led heri bør indgå en kritisk gennemgang af gældende regelsæt, en analyse af interne og eksterne kontrolmekanismer og eventuelt behov for at styrke disse, samt forslag til privatlivsfremmende løsninger, der kan anvendes i den offentlige sektor. Arbejdet bør munde ud i en sammenhængende og tidssvarende strategi for området med pilotforsøg på centrale områder.

PRIVACY KONSEKVENSANALYSE OG BRUG AF PRIVATLIVSFREMMENDE TEKNOLOGIER I OFFENTLIGE IT PROJEKTER

Retlige standarder og tekniske løsninger skal i højere grad sammentænkes. Dette kan blandt andet ske gennem privacy konsekvensanalyser (PIA), der foretages i forbindelse med opstart af nye offentlige IT projekter og lovforslag, der behandler persondata. Konsekvensanalyser indebærer blandt andet en proportionalitetsvurdering, risikovurdering, angivelse af tekniske og organisatoriske forholdsregler, og sikkerhedsforanstaltninger ved påtænkte overførsler til tredjeland, mv.

Privacy konsekvensanalyser er ikke obligatoriske i Danmark, mens de har i flere år været fast praksis for eksempel i Canada. Udgangspunktet i Canada er, at der foretages en risikovurdering med udgangspunkt i borgerens ret til beskyttelse. Det indebærer blandt andet, at borgeren ikke skal identificeres med mindre det er strengt nødvendigt i den

konkrete situation. Der er ligeledes udarbejdet detaljerede krav til, hvorledes disse analyser skal gennemføres og godkendes i samspil med den canadiske privacy kommissær. Den canadiske model kan tjene som inspiration for en dansk skabelon, idet der allerede er udarbejdet et omfattende materiale baseret på flere års erfaringer.

Ligeledes bør privacy som en naturlig og obligatorisk komponent tænkes ind i forbindelse med design af nye IT systemer (såkaldt "privacy by design"). Offentlige IT projekter bør i langt højere grad gøre brug af privatlivsfremmende teknologier, både ved nye IT løsninger men også når man skal gentænke for eksempel CPR løsning eller Nem-id.

For at sikre en reel styrkelse af databeskyttelsen i Danmark er det vigtigt, at arbejdsgruppens indsats munder ud i konkrete tiltag, der kan medvirke til at højne beskyttelsen af personoplysninger i både den offentlige sektor og blandt private virksomheder.

Institut for Menneskerettigheder anbefaler – med henblik på at fremme den enkeltes menneskerettigheder og imødekomme internationale anbefalinger:

- at der udarbejdes en samlet strategi for databeskyttelse og informationssikkerhed i Danmark.

- at tværfaglig rådgivning og tilsyn med databeskyttelse og informationssikkerhed styrkes, inklusiv rådgivning om brug af nye privatlivsfremmende teknologier.

- at privacy konsekvensanalyser indarbejdes som fast obligatorisk praksis i tilknytning til de ISO standarder (ISO27001) og den projektskabelon, som offentlige IT projekter skal følge;

- en styrket kontrol med offentlige IT projekter og leverandørers efterlevelse af de standarder for informationssikkerhed og databeskyttelse, der er foreskrevet i sikkerhedsbekendtgørelsen og ISO27001 standarden; og

- at privacy vurderinger udarbejdes i forbindelse med nye lovforslag på linje med analyse af miljømæssige eller økonomiske konsekvenser af lovforslaget.

Instituttet finder det positivt, at arbejdsgruppen vedr. databeskyttelse aktivt vil inddrage eksterne eksperter. I beretningen nævnes særligt Institut for Menneskerettigheder, Teknologirådet, Forbrugerrådet Tænk, Rådet for Digital Sikkerhed og Forbrugerombudsmanden. Da de nævnte problemstillinger spænder over både jura, tekniske løsninger,

og IT sikkerhed i bred forstand anbefaler instituttet, at der i den kommende proces foretages en bredere inddragelse af interessenter end disse fem organisationer, for eksempel gennem en række åbne, tematiske høringer.

Rikke Frank Jørgensen
FORSKER, PH.D

Arbejdsgruppen vedrørende datasikkerhed
under Retsudvalget
Att.: Birgitte Toft-Petersen

Sendt per email til: **Birgitte.Toft-Petersen@ft.dk**

IT-Politisk Forening
c/o Niels Elgaard Larsen
Århusgade 35, 1.
2100 København Ø

E-mail : bestyrelsen@itpol.dk
Web : http://www.itpol.dk

Dato : 29. august 2014

Høringsvar vedr. Beretning nr. 3 (nedsættelse af parlamentarisk arbejdsgruppe for datasikkerhed)

IT-Politisk Forening takker for muligheden for at afgive høringssvar om denne beretning fra Retsudvalget og Kulturudvalget. Vi er meget enige i, at der er behov for en bedre beskyttelse af borgernes persondata og deres ret til privatliv. Det gælder såvel i forhold til private virksomheder som offentlige institutioner.

Udvalgene planlægger at nedsætte to parlamentariske arbejdsgrupper, som forventes at beskæftige sig med en lang række emner fra logningsbekendtgørelsen, TV-overvågning, persondatabeskyttelse- og lovgivning, privacy by design til privacy impact assessments. Arbejdsgrupperne skal aflægge foreløbig rapport inden Folketingets åbning primo oktober, og en endelig rapport inden udgangen af 2014.

Efter vores vurdering er denne tidshorisont ikke realistisk, hvis arbejdsgrupperne skal producere en rapport med en substantiel analyse af de databeskyttelsesproblemer, som det danske samfund står over for, og hvis arbejdsgrupperne skal komme med konstruktive forslag til hvordan vi forbedrer forholdene på dette område.

Det er vores umiddelbare vurdering, at problemerne omkring persondatabeskyttelse i Danmark er ganske alvorlige, og at den aktuelle misbrugssag med Nets og Se og Hør reelt bare er toppen af isbjerget. Det skyldes flere ting.

På det offentlige område har vi i Danmark en lang tradition for store centrale databaser, hvor borgerne er registreret med CPR nummer. Der er samtidig stor velvillighed til at stille disse data til rådighed for andre offentlige myndigheder og andre formål end dem, som data oprindeligt er indsamlet til. Det betyder, at mange offentlige ansatte har adgang til ofte ganske følsomme oplysninger om borgerne. Det skaber en større risiko for misbrug, som man prøver at løse med kontrol og logning af adgangen til data.

Men der er også risikoen for at data lækkes fra systemerne ved en systemfejl, eller at hackere bryder ind i systemerne. De store centrale databaser, hvor CPR nummer altid er indgangen, gør konsekvenserne af systemfejl eller hacking langt værre. Brugen af CPR nummer i alle systemer gør det nemt at sammenkæde forskellige oplysninger om borgeren. Jo flere oplysninger om borgerne som hackere kan sammenkæde, desto større er risikoen for identitetstyveri eller andet datamisbrug.

Udformningen af de danske databaser med personhenførbare oplysninger er med andre ord ikke designet hensigtsmæssigt med henblik på den bedste beskyttelse af persondata. Man har ikke i tilstrækkelig grad indtænkt privacy i designet, og problemet vokser i og med antallet af centrale databaser er stigende.

En lang række nye og gamle opgaver er blevet digitaliseret på en sådan måde, at der er skabt nye centrale databaser med personhenførbare oplysninger, uden at der tages stilling til de deraf følgende risici for datamisbrug. De tre følgende 3 eksempler illustrerer dette udmærket:

1. Med klippekort og månedskort kunne borgerne bruge den offentlige transport uden at de enkelte rejser blev registreret. Med rejsekortet bliver borgernes rejser registreret på CPR-nummer niveau.
2. Vores el-målere skal erstattes af ”intelligente” el-målere, som kan fjernaflæses, og det er meningen at husstandens strømforbrug skal aflæses hver time. Disse oplysninger vil afsløre en masse detaljer om borgernes privatliv, f.eks. hvornår vi er hjemme.
3. Der er løbende overvejelser om roadpricing, og Trængselskommissionen har udarbejdet en rapport

om dette. Trængselskommissionens forslag ville imidlertid indebære en registrering af alle bilture i stil med rejsekortet, og altså en ny central registrering af borgernes færden i det offentlige rum.

Et fælles træk ved de tre eksempler er, at ingen tilsyneladende har overvejet om opgaven (betaling for offentlig transport, elektricitet eller roadpricing) kunne løses uden opbygning af store centrale databaser med persondata. Tværtimod virker det som om, at den nye registrering er blevet set som en helt naturlig udvikling i stedet for den betragtning, at den bedste beskyttelse af persondata består i at registrere så få persondata som muligt, og at registrere data der er så svært personhenførbare som muligt.

De tre eksempler er i virkeligheden forholdsvis trivielle i den forstand, at der eksisterer gode (sikre) løsninger, i hvert fald på proof-of-concept niveau. Men der er naturligvis mange andre databeskyttelsesproblemer i den offentlige sektor, som er langt sværere at løse. Det gælder ikke mindst sundhedsdata, specielt hvis man ønsker at bruge sundhedsdata til andre formål end behandlingen af borgerne, f.eks. forskning.

Problemerne er så komplekse, at det efter vores vurdering er nødvendigt at indrette de offentlige systemer efter andre principper end det sker i dag, hvor vi har store centrale databaser der let kan sammenkædes fordi CPR-nummeret er brugt overalt. De databeskyttelsesproblemer som vi står over for, kan ikke, på længere sigt, løses alene ved en bedre kontrol med adgangen til data.

I januar 2011 udgav IT- og Telestyrelsen en rapport ”Nye digitale sikkerhedsmodeller - et diskussionspapir”, som indeholdt mange visionære tanker om indretningen af offentlige IT-systemer. Vi er ikke bekendt med, at dette arbejde er blevet videreført efter 2011.

IT-Politisk Forening skal derfor opfordre til, at det tidligere arbejde med ”nye digitale sikkerhedsmodeller” kommer til at indgå i den brede afdækning som de to arbejdsgrupper forventes at udføre. Det vil falde naturligt ind under ”privacy by design”, som i forvejen er angivet blandt de ønskede arbejdsopgaver.

IT-Politisk Forening anmoder samtidig om at deltage i arbejdsgruppen vedrørende datasikkerhed under Folketingets Retsudvalg.

Referencer

”Nye digitale sikkerhedsmodeller - et diskussionspapir”, IT- og Telestyrelsen, januar 2011.
http://digitaliser.dk/resource/781482

25. aug. 2014

Dansk Journalistforbund
medier & kommunikation

The Danish Union of Journalists

Gammel Strand 46
1202 København K
Danmark

+45 3342 8000
dj@journalistforbundet.dk
journalistforbundet.dk

Til hhv.
Folketingets Kulturudvalg og
Folketingets Retsudvalg

fremsendes pr. mail

Dansk Journalistforbunds høringssvar vedrørende Kulturudvalgets og Retsudvalgets beretning nr. 3 afgivet den 3. juni 2014

Dansk Journalistforbund, DJ, har stor forståelse for og er enige i en lang række af de punkter, som Kulturudvalget og Retsudvalget nævner i sin beretning.

Først og fremmest er DJ helt enig i beretningens skarpe afstandtagen fra den overvågning og den anvendelse af personfølsomme oplysninger, der åbenbart har fundet sted. Der er tale om en ekstremt alvorlig krænkelse af de pågældende personers ret til et privatliv.

DJ har herudover følgende bemærkninger:

Arbejdsgruppen vedrørende datasikkerhed. Denne sag er kendt som Se og Hør-sagen. Men det er primært en sag om beskyttelsen af personfølsomme oplysninger og tilsynet med dette. Sagen handler først og fremmest om, at én eller få personer har kunnet overvåge og anvende nogle personfølsomme data, uden at dette er blevet opdaget. Dette må naturligvis ikke kunne ske.

Derfor er DJ også helt enig i de initiativer, som man oplister i beretningen vedrørende datasikkerhed: Der skal stilles større krav til beskyttelse af personfølsomme data, og der skal være et bedre tilsyn med efterlevelsen af disse krav.

DJ stiller sig til rådighed for at deltage i og/eller bidrage til det videre arbejde i arbejdsgruppen vedrørende datasikkerhed.

Arbejdsgruppen vedrørende medieetik og medieansvar. DJ finder det meget tilfredsstillende, at der i beretningen er entydige bemærkninger om vigtigheden af en fri og kritisk presse, og understregningen af det væsentlige i, at pressen har reel frihed til at kunne bringe også kritiske og afslørende historier.

DJ mener imidlertid ikke, at den aktuelle sag giver anledning til gennemgribende ændringer af de medieetiske og medieansvarsmæssige regler.

For det første er Se og Hør-sagen ganske åbenbart en helt usædvanlig kriminalsag, hvis omfang politiet og anklagemyndigheden arbejder på at belyse og i givet fald at føre til doms.
Efter DJ's opfattelse er det alt for vidtgående at lægge dette enestående eksempel til grund for at foreslå nogle meget markante stramninger af lovgivningen, som enkelte politikere har gjort.

For det andet er der de seneste år allerede sket en del på dette område:

- DJ har på et meget tidligt tidspunkt udtrykt ønske om – helt uafhængigt af verserende debatter – at opdatere de vejledende regler for god presseskik. I et samarbejde mellem DJ og Danske Medier blev dette arbejde gennemført i 2012-2013.
- En fokuseret kommunikationsindsats har bidraget til både at øge kendskabet til og forståelsen for Pressenævnets arbejde.
- Kulturudvalget og Retsudvalget holdt i maj 2012 en høring, hvor der netop var lejlighed til en grundig drøftelse af medieetik, mediernes ansvar mm.
- Endelig har Justitsministeriet i sin redegørelse fra 2013 til Retsudvalget og Kulturudvalget om niveauet for økonomisk kompensation (KUU Alm.del Bilag 152 og bilag 153) konkluderet, at der ikke aktuelt er anledning til at forhøje kompensationsniveauet for æreskrænkelser mv.

På den baggrund mener DJ ikke, at der umiddelbart er behov for ændringer i lovgivningen mv.

DJ har følgende bemærkninger til beretningens 3 punkter om medieansvar og medieetik:
Erstatningsansvar: Medieansvar er i høj grad mediernes ansvar, og helt overordnet støtter DJ fuldt ud den selvregulering, der foregår inden for medierne, og den lovgivning, der ligger til grund for denne regulering, herunder Medieansvarsloven.
Konkret er det DJ's opfattelse, at spørgsmålet om erstatning til personer, der udsættes for krænkelse af privatlivets fred, hører hjemme hos domstolene, og at der allerede eksisterer den fornødne lovgivning til at håndtere dette.

Betalte kilder: DJ finder, at det som udgangspunkt er i modstrid med god presseskik, hvis medier systematisk honorerer kilder for tips til gode historier, og DJ anbefaler derfor, at medierne ikke betaler tiphonorarer.
Det kan imidlertid være særdeles vanskeligt at opstille præcise regler og retningslinjer for dette.
For det første fordi det i praksis ikke er muligt konkret at definere grænsen mellem tipbetaling og betaling for det egentligt indhold.
For det andet kan der være situationer, hvor det altid vil være op til det enkelte medie selv at vurdere, hvilke journalistiske metoder, der skal anvendes for at sikre tilvejebringelsen af noget relevant og afgørende kildemateriale. I så fald vil det enkelte medies åbenhed om disse forhold være væsentlig for troværdigheden.
Endelig for det tredje er det DJ's opfattelse, at overordnede regler på dette område vil være i modstrid med selvreguleringen og dermed pressefriheden.

Gennemgang af praksis og normalstrafniveau: DJ henviser igen til den ovennævnte redegørelse fra Justitsministeriet (KUU Alm.del Bilag 152 og 153).

DJ ser frem til at kunne uddybe det ovenstående på det dialogmøde, som Kulturudvalget har indbudt til den 10. september 2014.
Hvis høringssvaret i øvrigt giver anledning til yderligere spørgsmål eller kommentarer, står DJ gerne til rådighed, mail DJ@journalistforbundet.dk.

Venlig hilsen

Mogens Blicher Bjerregård
formand

Tak for denne henvendelse!
Det står mig ikke helt klart, hvad der i forbindelse med høringen ønskes indhentet bemærkninger om. Så jeg vil indskrænke mig til at tilkendegive, at der ikke mindst i lyset af de seneste måneders begivenheder også efter min opfattelse har vist sig et åbenbart behov for at undersøge mulighederne for en bedre beskyttelse af personfølsomme oplysninger.
Venlig hilsen, Jørn Vestergaard

Jørn Vestergaard
professor i strafferet
Det Juridiske Fakultet
Københavns Universitet
Studiestræde 6
1455 København K

+45/21 60 26 80
jv@jur.ku.dk
http://jura.ku.dk/jv

NOTAT

Uddybning af KL´s holdning til EU's forordning om databeskyttelse

Den 29. august 2014

Sags ID: SAG-2014-04215
Dok.ID: 1900954

ASF@kl.dk
Direkte 3043 8254
Mobil 3043 8254

Weidekampsgade 10
Postboks 3370
2300 København S

www.kl.dk

Baggrund

Europa-Kommissionen har foreslået, at det nuværende persondatadirektiv[1] skal opdateres som en forordning. Persondatadirektivet er i Danmark implementeret via persondataloven.

Sagen er meget vigtig for kommunerne, som både behandler borgernes persondata som myndighed og persondata som arbejdsgiver for de ca. 500.000 kommunalt ansatte.

Den hastige digitale udvikling, som er sket siden 1995, har givet kommunerne helt nye muligheder for at yde borgerne bedre og hurtigere service - ikke mindst via digital selvbetjening. Og for KL er det væsentligt, at de nye muligheder ikke betyder dårligere sikkerhed omkring borgernes data.

I dette holdningspapir kan du læse KL's forslag til, hvordan borgernes og medarbejdernes data kan sikres på en måde, hvor borgerne reelt oplever en styrkelse af sikkerheden omkring deres data.

[1] (Direktiv 95/46/EF)

KL's holdning – kort fortalt

For at hverdagen skal kunne fungere for de danske kommuner, er det KL´s holdning, at forslaget til forordningen om databeskyttelse bør justeres væsentligt. Ifølge KL er der særligt fem temaer, som kræver opmærksomhed:

1. Forslaget til forordning gælder både den private og den offentlige sektor og vil harmonisere databehandling i alle medlemslandene. Det er uhensigtsmæssigt, da forordningsforslaget ikke tager højde for den offentlige sektors særlige opgaver samt den i forvejen høje grad af regulering af den offentlige sektors håndtering af persondata.

   – KL arbejder derfor for, at en kommende regulering sikrer den nødvendige fleksibilitet for den offentlige sektor.

2. På det ansættelsesretlige område giver forslaget til forordning ikke rum for den danske aftalemodel.

   – KL arbejder derfor for at sikre rum for den danske aftalemodel.

3. Der lægges op til meget administrativt tunge regler, som ikke ser ud til at tilføje værdi for borgerne i et omfang, der opvejer omkostningerne.

   – KL arbejder derfor for, at der er en rimelig balance mellem de nye administrative byrder og den datasikkerhed de nye regler giver borgerne.

4. Der lægges op til meget høje bøder i forslaget til forordning.

   – Det ønsker KL ændret og arbejder derfor for, at det skal være op til medlemslandene at beslutte, hvilke sanktioner de offentlige myndigheder pålægges.

5. Forslaget til forordning indeholder en lang række delegerede retsakter og uklare formuleringer, som skaber utryghed og usikkerhed for både borgere og myndigheder ift., hvad der er det gældende regler.

   – KL arbejder derfor for at sikre en klar lovtekst, der vil give både myndigheder og borger større tryghed.

De fem temaer uddybes i de følgende afsnit.

Tema 1 - Fleksibilitet for den offentlige sektor

KL's holdning er, at forordningsforslaget rammer uhensigtsmæssigt i forhold til offentlige myndigheder og i forhold til det ansættelsesretlige område, hvor hovedparten af de persondatabehandlinger, der foretages, er rent nationale. Reglerne i forordningen, fx retten til at blive glemt, er i vidt omfang udformet med henblik på at løse problemer, som omhandler internethandel, sociale netværk og dataoverførsler på tværs af landegrænser, hvor det er rigtigt, at en forordning, der gælder for alle virksomheder i EU, vil være en hensigtsmæssig reguleringsform.

Virksomheder behandler persondata med henblik på at opnå profit. Kommunerne indsamler persondata med henblik på at yde service til borgerne og ansætte medarbejdere. Det følger af offentligretlige grundsætninger, at kommuners behandling af oplysninger skal være saglig og proportional.

I dansk lovgivning findes endvidere en række særregler, der regulerer den offentlige sektors behandling af personoplysninger. Fx er behandling af personnumre i dag reguleret i persondataloven - ligesom der også er en særlig beskyttelse af oplysninger om væsentlige, sociale problemer og andre private forhold, som ikke i forordningen er karakteriseret som følsomme oplysninger. Der er ligeledes en række særlige regler i dansk lovgivning, der regulerer behandling af personoplysninger på det sociale område og på sundhedsområdet.

Europa-Parlamentet støtter Kommissionens forslag om en forordning. Rådet har endnu ikke lagt sig fast på reguleringsform.

KL støtter derfor den danske regering i, at det i en kommende regulering af behandling af persondata skal sikres, at medlemslandene for den offentlige sektor kan fastsætte nationale regler, der regulerer behandling af personoplysninger på særlige områder.

KL foreslår derfor, at den nødvendige fleksibilitet for den offentlige sektor skal sikres, og KL mener, at den nødvendige fleksibilitet sikres bedst ved et direktiv for den offentlige sektor. Det nuværende forordningsforslag er målrettet den private sektor.

Den offentlige sektor er i EU-landene meget forskelligt opbygget, fx er det ikke alle som har et cpr-register. Det gør, at der er store forskelle på, hvordan forordningen om databeskyttelse vil ramme de enkelte medlemslande.

En forordning og et direktiv er to meget forskellige retlige instrumenter. Kort sagt gælder en forordnings bestemmelser direkte og umiddelbart i medlemslandene, uden at der skal vedtages national lovgivning. Direktiver fastlægger som udgangspunkt et mål, der skal nås, men det er overladt til medlemslandene selv at bestemme form og midler til gennemførelse af direktivet, fx om direktivet skal gennemføres ved lov eller bekendtgørelse. Et direktiv vil derfor give medlemslandene et større råderum i forhold til at tilpasse lovgivningen de nationale forhold.

Tema 2 – sikre rum for den danske model

Hvis Kommissionens forslag til forordning vedtages, vil det være vanskeligt at bevare den danske arbejdsmarkedsmodel, og der vil fx ikke ved kollektiv aftale kunne vedtages en mere vidtgående beskyttelse af personoplysninger. Endvidere vil det ikke være muligt at opretholde den måde, man håndterer personoplysninger i ansættelsesforhold i dag.

Europa-Parlament har forsøgt at imødekomme arbejdsmarkedets parters kritik af Kommissionens forordning og Europa-Parlamentets forslag åbner derfor op for, at medlemsstaterne kan tillade, at der kan vedtages specifikke bestemmelser vedrørende ansættelsesforhold i kollektive overenskomster. Det fremgår dog samtidig, at det skal ske i overensstemmelse med bestemmelserne i forordningen og under overholdelse af proportionalitetsprincippet.

Derudover fremgår det af Parlamentets forslag, at hvis der vedtages nationale bestemmelser vedrørende behandling af oplysninger i ansættelsesforhold, skal disse bestemmelser leve op til en række minimumsnormer.

Selvom det er positivt, at de kollektive overenskomster er nævnt, er det KL's holdning, at Europa-Parlamentets forslag er for uklart, og det er stadig

usikkert, om arbejdsgiveres behandling af persondata i ansættelsesforhold fortsat kan forhandles ved kollektive overenskomster.

KL mener, at Danmark skal have mulighed for at opretholde det kollektive arbejdsretlige aftalesystem, som det kendes i dag. Det skal sikres, at rammerne for behandling af personoplysninger i ansættelsesforhold kan aftales ved kollektive overenskomster, således at arbejdsmarkedets parter fortsat kan mere vidtgående beskyttelsesforanstaltninger.

Det er ligeledes meget væsentligt for KL, at arbejdsgiverens ledelsesret ikke begrænses. KL lægger meget vægt på, at datasikkerheden sikres i kommunerne, og KL er enig i, at det i nogle tilfælde kan være hensigtsmæssigt - som det foreslås i forordningsforslaget - at ansætte en databeskyttelsesansvarlig, men KL finder, at det bør være op til den enkelte myndighed at beslutte, hvordan opgaven vedrørende databeskyttelse skal organiseres.

KL foreslår derfor, at det skal være frivilligt, om der skal ansættes en databeskyttelsesansvarlig, ligesom KL ikke finder, at den databeskyttelsesansvarliges opgaver skal reguleres i detaljer i en forordning. KL foreslår endvidere, at det klart fremgår, at behandling af personoplysninger kan ske på grundlag af et samtykke i ansættelsesforhold, og at rammerne for behandling af oplysninger kan aftales ved overenskomst.

En forordning vil betyde, at de aftaler, der i dag forhandles mellem LO/DA og KL/KTO ikke vil kunne opretholdes. I dag kan arbejdsmarkedets parter aftale at vedtage mere vidtgående beskyttelsesforanstaltninger af personoplysninger end det, som er angivet i det nuværende direktiv. Fx har arbejdsmarkedets parter via KTO´s kontrolaftale aftalt krav om længere varsling ved iværksættelse af kontrolforanstaltninger end de krav, som i dag bliver udstukket af det nuværende databeskyttelsesdirektiv.

Tema 3 – reel datasikkerhed frem for mere administration

Formålet med forordningsforslaget er, at der skal være større sikkerhed omkring borgernes data, sådan at borgerne oplever større tryghed ved at overlade deres data til private og offentlige aktører.

Borgerne har allerede stor tiltro den offentlige sektors behandling af deres data. KL mener derfor, at behovet for større datasikkerhed primært handler

om den private sektor. Den offentlige sektor er allerede reguleret af en lang række love, fx forvaltningsloven, cpr-loven og sundhedsloven, som sikrer, at borgerne kan være trygge ved at overlade deres data til det offentlige.

Tal fra Danmarks Statistik viser, at 94 % af de danske internetbrugere føler sig trygge ved at indsende blanketter eller indtaste personlige oplysninger på de offentlige myndigheders hjemmesider.

Derimod er det hver tredje internetbruger, som undlader at indtaste personlige oplysninger på sociale eller professionelle online netværkstjenester pga. utryghed i forhold til, hvad der sker med deres data.

Samtidig er det KL´s holdning, at forordningsforslaget lægger op til samme form for pseudodatasikkerhed som "Cookie-direktivet". Forordningen tager udgangspunkt i tanken om, at jo flere oplysninger borgerne gives om behandlingen af deres data, og jo flere gange borgerne skal give deres samtykke -fx ved at klikke "ok" på en hjemmeside, jo tryggere føler borgeren sig.

Fakta er, at borgerne springer de mange informationer om behandlingen af deres data over - både på papirblanketter og i selvbetjeningsløsninger. Og at klikke "ok" for at få adgang til fx en selvbetjeningsløsning blot gør borgeren irriteret.

Når det samtidig er særdeles omkostningsfuldt for kommunerne at give borgerne alle disse oplysninger uopfordret og indarbejde samtykkefunktioner i alle selvbetjeningsløsninger, kan KL kun være utilfredse med forordningens øgede oplysnings- og samtykkekrav.

I dag forventer borgerne tværtimod af den offentlige sektor, at når borgerne én gang har afgivet oplysninger fx i forbindelse med en sag, så kan alle dele af den offentlige sektor tilgå disse oplysninger og bruge dem i forbindelse med fx en ny sag. I regi af den fællesoffentlige digitaliseringsstrategi arbejdes der intenst på at tilvejebringe et sæt "grunddata" om borgere og virksomheder, som alle offentlige myndigheder kan anvende i forbindelse med deres sagsbehandling.

Forordningen understøtter ikke disse visioner, og dette skyldes i høj grad, at EU-Kommissionen har glemt at indtænke, hvordan den offentlige sektor arbejder. KL ønsker, at der skabes en balance mellem modernisering og effektivisering af sektoren og et fælles ønske om sikkerhed omkring borgernes data. Det er ikke nok, at Kommissionen har fokus på "den

digitale økonomi" - "den effektive, digitale offentlige sektor" bør også komme i spil.

Et andet eksempel er, at kommunerne på både beskæftigelsesområdet og social- og sundhedsområdet bruger såkaldt profilering af borgerne for at kunne hjælpe borgerne hurtigst muligt med at blive raske eller komme i arbejde. Profilering (digital udarbejdelse af en profil på borgeren) medvirker til at kunne give borgerne en individuel og målrettet indsats. Forordningsforslaget lægger op til, at dette ikke skal være muligt i en form, som er brugbar for kommunerne. Efter KL´s vurdering vil dette være et væsentligt tilbageskridt for mulighederne for at modernisere og forbedre kommunernes indsats for at hjælpe borgerne.

Når forordningsforslaget så oveni stiller krav om, at kommunerne bl.a. skal udarbejde såkaldte "konsekvensanalyser" af deres it-systemer. Det er KL´s erfaring, at disse ikke er de mange penge værd, som det vil koste kommunerne at udarbejde disse analyser. Det er derfor på tide at efterlyse "value for money".

At forordningen også kræver, at kommunerne skal opretholde indholdet i den nugældende, effektløse anmeldelsesordning ved fortsat at skulle udarbejde særskilt skriftlig dokumentation for alle behandlinger af persondata gør ikke tingene bedre. Og nye krav til indretningen af kommunernes it-systemer og blanketter giver heller ikke borgerne synligt bedre datasikkerhed i en offentlig sektor, hvor brud på datasikkerheden sker sjældent og alene skyldes menneskelig uagtsomhed.

KL vurderer, at borgerne er meget trygge ved den offentlige sektors behandling af deres data, og at forslaget til forordningen ikke i væsentlig grad vil øge sikkerheden omkring borgernes data, men blot fordyre kommunernes administration.

KL mener, at vejen frem i stedet er mere uddannelse af de kommunale medarbejdere, der behandler persondata som en del af deres arbejde. Idéen om at have en databeskyttelsesansvarlig ansat til særskilt at holde fokus på datasikkerheden i den enkelte myndighed synes KL også er en god idé. Blot mener KL ikke, at dette skal være et krav, men at kommunerne skal have mulighed for at organisere deres arbejde med datasikkerhed, som det passer bedst til den enkelte kommunes organisation.

Forslaget til forordning vil besværliggøre og fordyre realiseringen af potentialerne i den fællesoffentlige digitaliseringsstrategi særligt ift. kommunikationen med borgerne, da kommunerne skal indrette deres it-løsninger efter de ovenstående krav.

KL foreslår derfor, at kravene til behandlingen af borgernes data bliver proportional med den øgede sikkerhed og den tryghed som borgerne vil opleve.

Tema 4 - lavere bøder

Kommissionen foreslår dernæst et uforholdsmæssigt højt bødeniveau i forordningen.

Det betyder, at de danske kommuner, hvis de laver fejl, og dermed ikke overholder reglerne, vil kunne blive straffet med bøder på 250.000 EUR (1.875.000 kr.), hvis reglerne om den registreredes rettigheder ikke overholdes og bøder på 1.000.000 EUR (7.500.000 kr.), hvis der ikke udpeges en databeskyttelsesansvarlig.

Europa-Parlamentet er også her enig med Kommissionen i, at de nationale databeskyttelsesmyndigheder skal kunne give effektive sanktioner i tilfælde af lovbrud. Europa-Parlamentet har både lempet sanktionerne ved at foreslå brug af advarsler og periodiske revisioner, men også styrket sanktionerne ved at foreslå bøder til virksomheder på 100.000.000 EUR eller 5 % af den årlige omsætning.

KL mener, at Kommissionen og Europa-Parlamentet har haft internetgiganterne, de sociale medier og de store virksomheder, der benytter borgernes data med henblik på profit, for øje med denne forordning. De har således ikke taget højde for, at kommunerne indsamler borgernes data for at hjælpe borgeren og i borgerens interesse - og ikke med profit for øje. Samtidig er det vigtigt at understrege, at kommunerne ikke tjener penge på eventuelle sikkerhedsbrud. Men hvis persondata ulovligt udnyttes for kommerciel vinding skyld kan høje bøder give mening.

Det er yderst beklageligt, når der sker fejl i behandlingen af persondata og der skal gøres alt for, at det ikke sker. Menneskelige fejl kan dog ikke helt undgås. Det er derfor tvivlsomt, om et så højt bødeniveau vil give borgeren en bedre sikkerhed for, at der ikke sker brud ved behandlingen af dennes persondata.

KL foreslår derfor, at sanktionerne lempes og tilpasses konsekvenserne af de fejl, der eventuelt begås. KL foreslår desuden, at det bør være op til medlemsstaterne selv at fastsætte sanktionerne ved brud på lovgivningen - på samme måde som i det nugældende persondatadirektiv.

Tema 5 – klarere regler

Kommissionen har i forslaget til forordningen givet sig selv bemyndigelse til at udstede nye regler (delegerede retsakter) med krav til databeskyttelsen efter forordningens vedtagelse. Helt praktisk betyder det, at Kommissionen efterfølgende vil have mulighed for at "efterjustere" lovgivningen, og det vil betyde, at de investeringer som kommunerne har gjort for at efterleve forordningen kan være spildt, hvis der efter et år kommer et nyt lovgrundlag der fx kræver andre foranstaltninger for at afgive samtykke i elektroniskform.

Desuden indeholder forordningsforslaget en række uklarheder, som åbner op for at lovgivningen kan fortolkes på flere forskellige måder. Det er hverken myndigheder eller borgerne tjent med.

Europa-Parlamentet går imod Kommissionen på dette punkt, da det ikke mener, at Kommissionen skal have mulighed for efterfølgende at kunne justere i lovgivningen.

KL vurderer, at uklarhederne i forordningsforslaget vil skabe usikkerhed og uforudsigelighed om, hvordan datahåndteringen skal foregå. Eksempelvis medfører forordningen, at borgeren skal have en "garanti" for afgivet samtykke. Det er uklart, hvordan garanti skal forstås, og om det vil medføre en yderligere administrativ opgave for kommunerne.

KL mener, at det er uhensigtsmæssigt, hvis Kommissionen får mulighed for at udstede delegerede retsakter. Det vil medføre usikkerhed om, hvad der er og vil blive gældende ret. Konsekvenserne kan blive, at der efterfølgende indføres yderligere krav til kommunerne. Dette kan både blive dyrt, hvis det betyder krav om nye it-løsninger eller administrative procedurer og kan forsinke arbejdet med digitaliseringen af den offentlige sektor i regi af den fælleskommunale og fællesoffentlige digitaliseringsstrategi.

KL foreslår derfor, at reglerne gøres klare og letforståelige fra begyndelsen af. Det vil mindske behovet for at bruge delegerede retsakter. Kommissionens muligheder for efterfølgende at udstede delegerede

retsakter bør fjernes, ligesom uklarhederne i lovgivningen bør udbedres.

Det er KL's opfattelse, at hverken Kommissionen eller Europa-Parlamentet har leveret en klar lovgivningstekst i forhold til, at lovgrundlaget er en forordning – og derfor skal være meget klar. Derfor er det vigtigt, at Rådet tager den tid, der skal til for at sikre et klar lovgrundlag, som ikke åbner op for alt for mange fortolkningsmuligheder.

Folketingets Retsudvalg
Att. Birgitte.Toft-Petersen@ft.dk

Høringssvar vedrørende beretning nr. 3

Den 29. august 2014

Sags ID: SAG-2014-04215
Dok.ID: 1899549

LPJ@kl.dk
Direkte 3370 3160
Mobil 2327 1393

Weidekampsgade 10
Postboks 3370
2300 København S

www.kl.dk

Folketingets Retsudvalg har ved mail af 26. juni 2014 anmodet om KL's bemærkninger til beretning nr. 3 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.

KL er enig i, at det til stadighed er nødvendigt og relevant at se på, hvordan vi bedst sikrer borgernes data. Den digitale udvikling går stærkt. Og det er vigtigt, at borgerne har tillid til, at deres personlige oplysninger ikke falder i hænderne på de forkerte.

I forhold til arbejdsgruppens konkrete fokusområder skal KL gøre opmærksom på, at der er store problemer ved EU-Kommissionens forslag til forordning om databeskyttelse, som efter KL´s vurdering ikke i væsentlig grad vil øge sikkerheden omkring borgernes data, og som ikke tager højde for forskellene mellem den offentlige og den private sektors behandling af persondata. Samtidig spænder forordningsforslaget ben for udnyttelsen af de digitale muligheder til udvikling af den offentlige sektor med henblik på at kunne opretholde god service til borgerne.
./. KL´s holdning til de nye regler er uddybet i vedlagte notat.

KL finder, at vi allerede i dag har de nødvendige regler for beskyttelse af data. Udfordringen ligger i, hvordan vi i fællesskab sikrer reglerne overholdt – både via uddannelse, øget kontrol og ledelsesmæssigt fokus på datasikkerheden. KL vil derfor anbefale, at den nye arbejdsgruppe under Retsudvalget navnlig har fokus på, hvordan kendskabet til de allerede gældende regler for databeskyttelse generelt udbredes, bl.a. via en styrkelse og udvidelse af Datatilsynets opgaver.

Det hedder i beretningen, at arbejdsgruppen vil inddrage tekniske og juridiske eksperter i arbejdsgruppens arbejde. KL anbefaler, at kredsen af eksperter der er tiltænkt at indgå i arbejdet udvides, og KL stiller sig gerne til rådighed for udvalgets arbejde. Der behandles dagligt mange personoplysninger i kommunerne, og KL og kommunerne har stort fokus på sikkerheden omkring disse data. KL finder det derfor hensigtsmæssigt for udvalget arbejde, at også KL inddrages i arbejdsgruppens arbejde, således at den kommunale viden og erfaring kommer til at indgå i arbejdsgruppens afdækning af området.

Udover de tekniske og juridiske aspekter af sagen finder KL også, at det er afgørende, at der lægges vægt på såvel de økonomiske konsekvenser som de forvaltningsmæssige konsekvenser af implementering af arbejdsgruppens anbefalinger.

Med venlig hilsen

Pia Færch
Kontorchef

Emne: SV: Høring om beretning nr. 3 fra arbejdsgruppen om datasikkerhed under Folketingets Retsudvalg - høringssvar fra Konkurrence- og Forbrugerstyrelsen

Konkurrence- og Forbrugerstyrelsen har den 26. juni 2014 modtaget høringsmateriale fra Folketingets Udvalgssekretariat på vegne af arbejdsgruppen om datasikkerhed under Folketingets Retsudvalg. Høringsmaterialet består i beretning nr. 3 (uden bilag) og brev fra arbejdsgruppens formand.

Høringsmaterialet drejer sig 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.

Konkurrence- og Forbrugerstyrelsen har ikke bemærkninger til beretningen.

Styrelsen skal blot overordnet gøre opmærksom, at de konkrete initiativer – fx i forhold til lovgivning – der måtte blive resultatet af udvalgsarbejdet, forudsættes at leve op til bl.a. grundlæggende principper om lige, objektive og ikke-diskriminerende vilkår.

Med venlig hilsen

Sigurd Slot Jacobsen
Specialkonsulent/Special Advisor
Konkurrence- og Forbrugerstyrelsen/
Danish Competition and Consumer Authority
Direkte +45 4171 5271
E-mail ssj@kfst.dk

KONKURRENCE- OG FORBRUGERSTYRELSEN
Carl Jacobsens Vej 35
2500 Valby
Tlf. +45 4171 5000

Vi arbejder for velfungerende markeder

Københavns Byret

Folketinget
Retsudvalget
Christiansborg
1240 København K

Præsidenten
Domhuset, Nytorv 25
1450 København K.
Tlf. 99 68 70 15
CVR 21 65 95 09
administration.kbh@domstol.dk
J. nr. 9099.2014.28

Den 13. august 2014

Ved en mail af 26. juni 2014 har Folketinget anmodet om bemærkninger til beretning nr. 3 afgivet af Folketingets Kulturudvalg og Retsudvalg 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.

Jeg skal i den anledning på byretspræsidenternes vegne oplyse, at beretningen ikke giver byretterne anledning til at fremkomme med bemærkninger.

Med venlig hilsen

Søren Axelsen

Landsorganisationen i Danmark
Danish Confederation of Trade Unions

Islands Brygge 32D
Postboks 340
2300 København S

Telefon 3524 6000
Fax 3524 6300
E-mail lo@lo.dk

Retsudvalget
Att.: Birgitte Toft-Petersen

birgitte.toft-petersen@ft.dk

Sagsnr. 14-1774
Vores ref. PLE/lhaa
Deres ref.

Den 14. august 2014

Høring over beretning 3

Ved skrivelse af 25. juni 2014 har Retsudvalget sendt ovennævnte beretning i høring.

Det kan oplyses, at LO ikke har bemærkninger til denne.

Med venlig hilsen

Pernille Leidersdorff-Ernst

POLITI FORBUNDET

Folketinget
Retsudvalget
Christiansborg
1240 København K
Att.: Birgitte Toft-Pedersen

Sendt pr. mail:
Birgitte.Toft-Pedersen@ft.dk

Journalnr. 2014-00596
30. juli 2014
HB/kg

Vedrørende høring over beretning nr. 3

Tilbagesendes til Folketingets Retsudvalg, idet Politiforbundet som sådan ikke har bemærkninger til høringen. Imidlertid henledes opmærksomheden på, at man bør sikre, at der ikke gives bedre muligheder for beskyttelse af personfølsomme oplysninger i omtalte type af sager, end der eksempelvis kan ydes for at beskytte forbundets medlemmer (polititjenestemænd) for offentliggørelse i henhold til offentlighedsloven. Politiforbundet har i den forbindelse hæftet sig ved, at Ombudsmanden i sin afgørelse fra den 3. juli kraftigt har kritiseret Ministeriet for Børn, Ligestilling Integration og Sociale forhold, for ikke at givet en journalist aktindsigt i de sagsbehandlende medarbejderes navne (den såkaldte Lisbeth Zorning sag). Baggrunden er at aktindsigt kun kan afslås efter § 33, stk. 5, hvis der er nærliggende fare for, at de nævnte interesser vil lide skade af betydning. Praksis viser imidlertid, at det kun er i ganske få særlige tilfælde, det således er muligt at beskytte den enkelte ansatte. Det vil sige, at der skal være tale om helt konkret risiko og/eller mistanke om, at medarbejderen ved aktindsigten/offentliggørelsen udsættelse for strafværdig chikane.

På forbundets vegne - og med venlig hilsen

Hans Bundesen
Seniorkonsulent

H.C. Andersens Boulevard 38 · DK-1553 København V · Tlf. +45 3345 5900 · Fax +45 3345 5901
mail@politiforbundet.dk · www.politiforbundet.dk

R E T S P O L I T I S K F O R E N I N G

Retspolitisk Forenings kommentar til udkast til beretning nr. 3 fra Folketingets Retsudvalg og Kulturudvalg.

Indledende bemærkninger og problemstilling.

Retspolitisk Forening (RPF) har noteret sig, at udvalgenes overvejelser tager udgangspunkt i sagen om videregivelse og offentliggørelse af fortrolige oplysninger i ugebladet Se og Hør. Således som Foreningen vurderer problemstillingen også i udgangspunktet, er den langt bredere og omfatter enhver registrering, behandling og videregivelse af personfølsomme oplysninger. Dette synes da også at kunne læses ud fra de bemærkninger udvalgene er fremkommet med under afsnittet "politiske bemærkninger", hvori det bl.a. hedder:

" At regeringen pålægges at udvide det af ministeren nedsatte tværministerielle embedsmandsudvalg, der skal kortlægge sikkerhedsproblemer, for så vidt angår betalingskort m.v., til at omfatte alle områder, hvor der opbevares personfølsomme oplysninger og data. Dette kan eventuelt ske i flere etaper, hvor forskellige områder afdækkes løbende, så hastigheden fremmes".

Tillige kan navnlig de efterfølgende pålæg til regeringen forstås som en erkendelse af, at problemstillingen er langt bredere og væsentligt mere kompliceret end et om end klart retsstridigt brud på fortrolighedsreglerne for NETS. Det hedder bl.a, at regeringen: skal

" ..aktivt at arbejde for, at persondatabeskyttelsen vægtes højt i det kommende EU-direktiv/ forordning på databeskyttelsesområdet. Regeringen opfordres til at samarbejde aktivt med bl.a. Tyskland og Frankrig, der i modsætning til Danmark har været særdeles aktive i den forløbne proces, for så vidt angår sikringen af personfølsomme data, herunder offentlige data".

Et brud på de gældende regler, således som det er sket i Se og Hør sagen, er i realiteten umuligt at gardere sig i mod, men skal naturligvis retsforfølges. Det skal desuden bemærkes, at konsekvensen af disse ulovlige handlinger både for så vidt angår NETS og Se og Hør forekommer behersket, objektivt set uinteressant og forholdsvis uskyldigt. Hvorvidt et medlem af kongehuset har benyttet sit kreditkort et eller andet sted i verden, synes at være en oplysning, der hverken er særligt overraskende eller interessant ud fra en generel synsvinkel

om beskyttelse af privatlivets fred. Se og Hørs brug af oplysninger fra NETS kan sammenlignes med videregivelse af såkaldte trafikdata, men i de mange tilfælde, hvor Se og Hør har benyttet oplysningerne, har anvendelsen været kendt, idet de benyttede data har været grundlag for offentliggørelse af journalistisk bearbejdede meddelelser. Dette indebærer selvsagt ikke en accept af de begåede ulovligheder, men retter fokus mod den behandling og videregivelse, der finder sted på et helt lovligt grundlag.

EU's arbejde med et nyt direktiv om databeskyttelse må imidlertid forventes kun i særdeles begrænset og kun indirekte omfang at tage stilling til indsamling, bearbejdning og videregivelse af data indsamlet af medlemslandendes efterretningstjenester eller retshåndhævende myndigheder, da disse myndigheders virksomhed ikke umiddelbart er omfattet af unionens traktatbestemmelser og derfor heller ikke er dækket af bestemmelserne i unionens menneskerettighedscharter.

RPF læser opgavebeskrivelsen i beretningsudkastet s. 2 for de foreslåede parlamentariske arbejdsgrupper, således, at disse alene skal tage stilling til indsamling, behandling og videregivelse af personoplysninger, der befinder sig i private eller koncessionerede databaser. Det anføres således:

" afdækning af beskyttelsen af borgernes personfølsomme oplysninger og forventes konkret at se på i hvert fald følgende områder:
– Logningsreglerne og personoplysningsloven.
– EU's nye databeskyttelsesforordning og forbedringer af persondataloven, herunder retten til at blive glemt på nettet.
– Eksternt tilsyn med overholdelse af gældende lovgivning, herunder Datatilsynets kompetencer og ressourcer, samt andre tilsynsorganer af relevans for området og behovet for eventuel oprettelse af nye organer.
– Behovet for samling af it- og datasikkerhed ved en ansvarlig ressortminister.
– Internt tilsyn, herunder sikkerhedsgodkendelse af personer med adgang til personfølsomme data, samt opdeling af medarbejdere i flere sikkerhedsniveauer, der regulerer adgangen til oplysninger.
– Erfaringen med anonymisering af data, således at fordelene ved store datasæt til brug f.eks. forskning eller
kommerciel udnyttelse af big data ikke umuliggøres, men at det samtidig sikres, at data ikke kan føres tilbage til en kendt identitet."

Retspolitisk Forening finder det væsentligt og positivt, at udvalgene er opmærksomme på disse problemstillinger, men skal tillige anføre, at de angivne problemstillinger ikke forekommer dækkende for behovet for en grundig bearbejdning af samtlige spørgsmål, der vedrører data, der omfatter oplysninger, der kan henføres til grundlovens bestemmelser om brud på meddelelseshemmeligheden (§ 72), der alene hjemler en *særegen* lovfæstet undtagelse fra kravet om retskendelse.

Foreningen skal herefter bemærke:

Offentligt indsamlede oplysninger, herunder oplysninger indhentet af efterretningstjenesterne. Den relevante lovgivning er lovene om politiets og forsvarets efterretningstjenester, lov om center for cybersikkerhed samt persondataloven.

> I tilslutning hertil bør tillige nævnes den såkaldte logningsbekendtgørelse, der forpligter teleselskaberne til opbevaring og registrering af ganske betydelige datamængder (ifl. Justitsministeriet alene i 2008 450 mia. posteringer). Logningsbekendtgørelsen ændres dog, således, at de såkaldte sessionslogninger (internetlogninger) glider ud. Det må imidlertid forventes, at bekendtgørelsen helt ændres som følge af EU-domstolens dom af 8. april 2014, der erklærer bekendtgørelsens underliggende EU-retsakt (det europæiske logningsdirektiv (2006/24/EC)) for et for omfattende og alvorligt indgreb i retten til privatlivets fred og ikke i tilstrækkelig grad tager hensyn til beskyttelse af personoplysninger.

1. Loven om Forsvarets Efterretningstjeneste

Forsvarets Efterretningstjeneste kan *indsamle og indhente* oplysninger, der *kan* have betydning for tjenestens efterretningsmæssige virksomhed (FE-lovens §3). Som udgangspunkt er persondataloven ikke gældende for tjenestens virksomhed. Tjenesten kan *behandle* enhver personoplysning vedrørende en i Danmark hjemmehørende fysisk person, hvis behandlingen…. må antages at have betydning for varetagelsen af tjenestens opgaver efter lovens § 1, stk. 1 og 4, eller er nødvendig for varetagelsen af tjenestens opgaver efter § 1, stk. 2. Disse opgaver er i lovteksten beskrevet bredt, men skal selvsagt forstås i lyset af tjenestens funktion som Danmarks udenrigsefterretningstjeneste og militære efterretningstjeneste.

Tjenesten kan *behandle* oplysninger vedrørende en i Danmark hjemmehørende fysisk person efter samme kriterier. *Videregivelse*, herunder videregivelse til udenlandske myndigheder og private, af sådanne oplysninger kan bl.a. ske, såfremt videregivelsen sker til varetagelse af private eller offentlige interesser, der klart overstiger hensynet til de interesser, der begrunder hemmeligholdelse, herunder hensynet til den, oplysningen angår. Bestemmelsen skal formentlig forstås i snæver forstand. Men til gengæld kan der i så fald også videregives private fortrolige oplysninger om strafbare forhold, politisk observans m.m.

Det vil i denne sammenhæng være væsentligt, at få præciseret, hvilket anvendelsesområde denne videregivelsesmulighed har, da de specielle bemærkninger til bestemmelsen i forslaget til lov om forsvarets efterretningstjeneste ikke forholder sig til dette spørgsmål.

Retspolitisk Forening anbefaler, at lovene om politiets og forsvarets efterretningstjenester ændres, således, at videregivelse af private fortrolige oplysninger uden samtykke til udenlandske myndigheder eller private fysiske eller juridiske personer alene kan som led i et ske internationalt samarbejde om forebyggelse og bekæmpelse af forbrydelser, der er strafbare i Danmark. Oplysninger, der kan indebære en risiko for tortur eller anden umenneskelig behandling, skal dog ikke kunne videregives.

Der har i offentligheden, efter RPF's opfattelse med rette, været fokus på *videregivelse* af såkaldte rådata, der kan indeholde oplysninger om danske statsborgere eller personer, der har lovligt ophold her i landet. Samarbejdet med udenlandske efterretningstjenester rejser en lang række problemer navnlig ved videregivelse af data vedrørende danske fysiske og juridiske personer. (FE)Lovforslagets bemærkninger (pkt. 4.4.3.) anfører herom, at der: " skal være mulighed at der for at videregive rådata, idet videregivelsen samtidig bør bero på en afvejning af behovet for at videregive og de risici, der kan være forbundet hermed. I forbindelse med videregivelse af rådata bør det derfor indgå som en afgørende faktor, om videregivelsen af data ka**n** indebære en risiko for tortur eller anden umenneskelig behandling. "I betragtning af, at der er tale om rådata, der netop er karakteriseret ved at være data, der hverken er erkendte eller behandlet, forekommer bemærkningerne om afgørende vægt på risiko for tortur m.m. i forbindelse med videregivelse at være et usikkert kriterium, da anvendelsen af en sådan faktor forudsætter en databehandling, som ikke finder sted.

Retspolitisk Forening anbefaler, at der i forbindelse med egen videregivelse eller bistand til videregivelse til udenlandske myndigheder eller private fysiske eller juridiske personer indsættes en spærring, således at oplysninger om danske statsborgere og herboende udlændinge med lovligt ophold, alene kan videregives som led i et ske internationalt samarbejde om forebyggelse og bekæmpelse af forbrydelser, der er strafbare i Danmark. Videregivelse af data, der kan indebære en risiko for tortur eller anden umenneskelig behandling, skal dog ikke kunne videregives. Dette indebærer, at trafikdata vedrørende den nævnte gruppe, må analyseres med henblik på at vurdere, hvorvidt videregivelse opfylder de nævnte betingelser.

2. Lov om Center for Cybersikkerhed.

Den nyligt vedtagne lov definerer i modsætning til dens forgænger en sikkerhedshændelse som: " En hændelse, der negativt påvirker *eller vurderes* at ville kunne påvirke tilgængelighed, integritet eller fortrolighed af data, informationssystemer, digitale netværk eller digitale tjenester. "Den oprindelige definition i L 197 (GovCert-loven) (2010-11 1. samling) § 3 lød: *"Sikkerhedshændelse:* Hændelse, der *påvirker* tilgængelighed, integritet eller fortrolighed af information eller tjenester på internettet. "Definitionen er altså betragteligt udvidet til nu også at omfatte *vurderede* hændelser. Centrets virksomhed er som

udgangspunkt ikke omfattet af persondataloven. Offentlighedsloven og forvaltningsloven finder i det væsentligste heller ikke anvendelse.

De data (såvel trafikdata som pakkedata), som centrets netsikkerhedstjeneste kommer i besiddelse af, kan bl.a. behandles når behandlingen vurderes at kunne bidrage væsentligt til Center for Cybersikkerheds muligheder for at sikre informations- og kommunikationsteknologisk infrastruktur, som samfundsvigtige funktioner er afhængige af (§§ 6 nr. 2 og 7 nr.2). *Behandling* af alle typer personoplysninger kan bl.a. finde sted ved begrundet mistanke om en sikkerhedshændelse jf. § 10 nr. 7. Tilsvarende gælder *videregivelse*. Videregivelse til udenlandske samarbejdspartnere kan dog kun finde sted for så vidt angår trafikdata eksempelvis navne, IP-adresser, betalingskorttransaktioner m.m.

Da Center for Cybersikkerhed er henlagt til FE, er der fri udveksling af oplysninger mellem netsikkerhedstjenesten og den øvrige del af efterretningstjenesten.
Retspolitisk Forening skal anbefale, at det overvejes, hvorvidt der er behov for den udvidede definition af en sikkerhedshændelse. Det bør tillige overvejes, hvorvidt der er behov for at undtage centrets virksomhed fra persondataloven og i stedet lade denne lov være gældende med de modifikationer, der følger af netsikkerhedstjenestens behov for effektivitet og samarbejde med danske og udenlandske myndigheder. Endelig forekommer det som et væsentligt spørgsmål, hvorvidt den givne begrundelse for placeringen under FE, synergieffekten, er tilstrækkelig fyldestgørende, når henses til behovet for at understøtte et højt informationssikkerhedsniveau i den informations- og kommunikationsteknologiske infrastruktur, som samfundsvigtige funktioner er afhængige af. Endelig bør det genovervejes, hvorvidt der er behov for de stærkt forlængede sletningsfriste eller, hvorvidt det er tilstrækkeligt at fastholde sletningsfristerne i GovCert-loven fra 2011.

3.Tilsynet.
Tilsynet med såvel forvaltningen af lovene om efterretningstjenesterne og lov om center for cybersikkerhed er henlagt til det nye tilsyn med efterretningstjenesterne, jf. § 16 i lov om Politiets Efterretningstjeneste. Dette tilsyn har kun beskedne beføjelser, og der er ikke nogen transparens i tilsynets virksomhed bortset fra en årlig redegørelse til forsvarsministeren.

Retspolitisk Forening skal anbefale, at tilsynet får mulighed for at give efterretningstjenesterne og Center for Cybersikkerhed pålæg vedrørende behandling af personoplysninger.

Endelig anbefaler foreningen, at der sker en generel kortlægning af omfanget af samarbejdet med udenlandske efterretningstjenester og IT-sikkerhedstjenester, herunder angivelser af omfanget af videregivne personoplysninger, herunder rådata. Kortlægningen skal tillige omfatte Center for Cybersikkerheds virksomhed fra oprettelsen i 2011 til ikrafttrædelsen af den nye lov.

København, den 28. august 2014

Bjørn Elmquist	Leif Hermann
Formand	Bestyrelsesmedlem

RIGSREVISIONEN

St. Kongensgade 45
1264 København K

Tlf. 33 92 84 00

rr@rigsrevisionen.dk
www.rigsrevisionen.dk

Til Formanden for arbejdsgruppen vedrørende datasikkerhed under Folketingets Kultur- og Retsudvalg, Karsten Lauritzen.
Att: Birgitte Toft Petersen, birgitte.toft-petersen@ft.dk

27. august 2014

Kontor: 14

J.nr.: 2014-1496-1

Rigsrevisionens høringssvar vedrørende Retsudvalgets beretning nr. 3.

1. Arbejdsgruppen vedrørende datasikkerhed under Retsudvalget har i mail af 25. juni 2014, anmodet om Rigsrevisionens bemærkninger til beretning nr. 3 afgivet af Folketingets Kulturudvalg og Retsudvalg. Beretningen vedrører nedsættelsen 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.

Rigsrevisionen har ikke bemærkninger til Kultur- og Retsudvalgets beretning nr. 3, men skal dog supplerende oplyse følgende:

2. Det er Rigsrevisionens opgave ved revisionen bl.a. at efterprøve og vurdere, om statslige virksomheders dispositioner er i overensstemmelse med love og andre forskrifter samt med indgåede aftaler og sædvanlig praksis. Herunder kan Rigsrevisionen fx undersøge, om virksomhederne efterlever persondatalovens bestemmelser.

3. På baggrund af tidligere udførte it revisioner er det Rigsrevisionens vurdering, at ikke alle statslige virksomheder har efterlevet persondatalovens bestemmelser. Rigsrevisionen skal i den forbindelse bl.a. henvise til ”Beretning om revision af statsregnskabet 2011”, afsnit III.C, side 32-37 og afsnit III.D, side 37-45, samt ”Beretning om revision af statsregnskabet for 2012”, punkt 37 og punkt 262. Begge beretninger er vedhæftet til orientering.

4. Rigsrevisionen vil endvidere afgive en beretning til Statsrevisorerne om udvalgte statslige virksomheders beskyttelse af personoplysninger og virksomhedsdata i nær fremtid. Rigsrevisionen forventer at afgive beretningen til Statsrevisorerne i efteråret 2014.

Beretningen omhandler bl.a. beskyttelse af personoplysninger hos Danmarks Statistik, der opbevarer mange typer af oplysninger om alle danskere, herunder nu afdøde, siden CPR nummerets indførelse. Ud over Danmarks Statistik omhandler beretningen beskyttelse af personoplysninger i udvalgte systemer hos Rigspolitiet, Forsvarskommandoen, SKAT, Institut for menneskerettigheder, Socialstyrelsen, Arbejdsskadestyrelsen og Sundhedsstyrelsen.

Med venlig hilsen
Peder Juhl Madsen
Kontorchef.

Hvidovre 28. august 2014

SikkerhedsBranchen har med glæde modtaget og læst beretning nr. 3, afgivet 3. juni 2014 af Kulturudvalget og Retsudvalget.

Det er svært at være uenig i de politiske bemærkninger om datasikkerhed, som skal være grundlag for de to parlamentariske arbejdsgruppers arbejde. Oplægget kommer godt rundt, og det er ambitiøst, ikke mindst med de tidsfrister, arbejdsgrupperne skal arbejde under.

En ændring af lovgivningen om datasikkerhed er en balance. Der skal være en høj sikkerhed, men lovgivningen skal også indrettes, så borgernes og lovgivernes daglige liv med dem ikke bliver unødig besværligt. Begge dele kalder på et styrket eksternt tilsyn og et styrket tilsyn med de, der har adgang til oplysninger om borgerne.

Her kan SikkerhedsBranchen varmt støtte idéen om certificering og registrering af alle opsatte overvågningskameraer. Forslaget var fremme allerede ved gennemførelsen af ændringen af Lov om tv-overvågning i 2007 (L 162, fremsat 28. februar 2007), og har været oppe ved de efterfølgende mindre ændringer af loven i 2010 og 2011. Forslagsstillerne havde samme bekymring som SikkerhedsBranchen havde og stadig har, at datasikkerheden ofte ignoreres, men at den kan forbedres betydeligt via en certificering.

Der eksisterer allerede en frivillig ISO 9001-certificering på området, som mange installationsfirmaer er med i, men mange mindre firmaer og alle private er uden for. Det er en alvorlig trussel mod datasikkerheden og retssikkerheden.

At der er et behov for opstramning, viser to sager, hvor Datatilsynet i 2011 inspicerede Greve og Vallensbæk kommuners tv-overvågning. I Greves tilfælde fremgik det af dagspressen, at besøget var varslet mere end en måned i forvejen. Det samme har formentlig været tilfældet med Vallensbæk. Datatilsynet fandt en del lovovertrædelser i begge kommuner. Når to så store organisationer med en måneds varsel ikke præsterer bedre, er der al mulig grund til at tro, at situationen ikke er bedre i en lille detailforretning eller i et boligområde.
Eksemplerne fra de to kommuner er beskrevet på Datatilsynets hjemmeside:
http://www.datatilsynet.dk/afgoerelser/arkiv-over-afgoerelser/artikel/greve-kommunes-brud-paa-persondataloven-i-forbindelse-med-tv-overvaagning/
http://www.datatilsynet.dk/afgoerelser/arkiv-over-afgoerelser/artikel/vallensbaek-kommunes-brud-paa-persondataloven-i-forbindelse-med-tv-overvaagning/

Registreringen af opsatte kameraer vil hjælpe Datatilsynet og politiet når det hurtigt skal finde optagelser. Hvis der indføres en registrering hos Datatilsynet, bør lovgivningen samtidig ændres,

Sekretariat: Sikkerhedens Hus • Jernholmen 12 • 2650 Hvidovre • Tlf. 36 49 40 80 • Fax 36 34 90 01
e-mail info@sikkerhedsbranchen.dk • www.sikkerhedsbranchen.dk

så Datatilsynet har påtalemyndighed for både Lov om tv-overvågning og Persondataloven, idet ekspertisen på området findes hos tilsynet. I dag har Datatilsynet kun påtalemyndighed for Persondataloven.

En ændret lovgivning, som stiller flere krav til Datatilsynet, må naturligvis betyde en øget bevilling til tilsynet. Det er vor opfattelse, at tilsynet allerede under den eksisterende lovgivning har behov for en øget bevilling.

Med disse bemærkninger skal SikkerhedsBranchen ønske arbejdsgrupperne held og lykke med de kommende travle måneder. Er der noget i dette brev, der kræver uddybning, eller har arbejdsgrupperne undervejs noget, de mener SikkerhedsBranchen kan hjælpe med, står vi naturligvis til rådighed.

Med venlig hilsen

Kasper Skov-Mikkelsen
SikkerhedsBranchen

DET JURIDISKE FAKULTET
KØBENHAVNS UNIVERSITET

Folketingets Retsudvalg
Formand for arbejdsgruppen vedr. datasikkerhed
Karsten Lauritzen

15. JULI 2014

STUDIEGÅRDEN
STUDIESTRÆDE 6, ST 02-0-06
1455 KØBENHAVN K

DIR +45 35323342
MOB +45 23231901

tb@jur.ku.dk
www.jura.ku.dk/trinebaumbach

Datasikkerhed

Ved brev af 25. juni 2014 har formanden for arbejdsgruppen vedrørende datasikkerhed under Retsudvalget anmodet om bemærkninger til beretning nr. 3 afgivet af Folketingets Kulturudvalg og Retsudvalg 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.

Det er særdeles positivt, at Kulturudvalget og Retsudvalget har taget initiativ til at nedsætte en parlamentarisk arbejdsgruppe under inddragelse af eksterne eksperter på dette overordentlig vigtige felt.

Det bemærkes i den anledning særligt, at medier omfattet af medieansvarsloven i vidt omfang ikke er omfattet af persondataloven, (jf. persondatalovens § 2, stk. 6, 9 og 10), og dermed ikke omfattet af Datatilsynets kontrol eller anden tilsvarende kontrol. Det synes derfor fornødent i overensstemmelse med Kulturudvalgets og Retsudvalgets ovennævnte beretning at foretage en nærmere granskning af, hvorvidt der er behov for en bedre beskyttelse af de personfølsomme oplysninger, som pressen er eller kommer i besiddelse af, og om der er behov for at etablere en effektiv kontrolinstans på dette felt.

Med venlig hilsen

Trine Baumbach
Lektor, ph.d.

Vestre Landsret
Præsidenten

Folketinget
Retsudvalget
att. Retsudvalgets arbejdsgruppe vedrørende datasikkerhed
Christiansborg
1240 København K.

J.nr. 40A-VL-24-14
Den 01/09-2014

Arbejdsgruppen vedrørende datasikkerhed under Retsudvalget har ved brev af 25. juni 2014 anmodet om bemærkninger til beretning nr. 3 afgivet af Folketingets Kulturudvalg og Retsudvalg om nedsættelse af en parlamentarisk arbejdsgruppe, der skal undersøge mulighederne for en bedre beskyttelse af personfølsomme oplysninger og et effektivt tilsyn med offentlig institutioner såvel som private virksomheders behandling af disse.

I den anledning skal jeg meddele, at beretningen ikke giver landsretten anledning til at fremkomme med bemærkninger.

Dette svar sendes efter anmodning pr. e-mail til Birgitte.Toft-Petersen@ft.dk.

Med venlig hilsen

Bjarne Christensen

Østre Landsret
Præsidenten

Den 13 AUG. 2014
J.nr. 40A-ØL-28-14
Init: cr

Folketinget
Retsudvalget
Christiansborg
1240 København K

Høringssvar er sendt pr. mail til birgitte.toft-petersen@ft.dk

Folketingets Retsudvalg har ved brev af 25. juni 2014 anmodet om eventuelle bemærkninger til beretning nr. 3 (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).

I den anledning skal jeg meddele, at beretningen ikke giver landsretten anledning til at fremkomme med bemærkninger.

Med venlig hilsen

Bent Carlsen

Ellen Busck Porsbo

IT-Branchen fremsender hermed kommentarer til høringen fra Rets- samt kulturudvalget omkring data-sikkerhed.

- IT-Branchen har med alvor fulgt Se&Hør-sagen, som den blandt andet er blevet udlagt i pressen. IT-Branchen har drøftet sagen med vores medlemmer og med offentligheden på debatarrangementer og møder, som IT-Branchen har afholdt.

- Der er enighed i IT-Branchens medlemskreds om, at Se&Hør-sagen baserer sig på en enkeltstående hændelse, hvor en medarbejder på egen hånd har udført strafbare handlinger. IT-Branchen mener således ikke, at Se&Hør-sagen er udtryk for et generelt problem blandt danske IT-virksomheder, der i forskellig grad håndterer personhenførbare data.

- IT-Branchen finder det relevant at skabe parlamentarisk fokus på den eksisterende retstilstand, tilsyn og sanktionsbeføjelser for at øge sandsynligheden for, at lignende hændelser ikke opstår i fremtiden, og for at sikre, at misbrug af data hurtigt vil blive opdaget, standset og straffet.

- Det er IT-Branchens opfattelse, at der ikke er behov for mere politisk regulering end de omfattende regler, der er på området i dag. Det kan derimod ikke afvises, at der måtte være behov for at præcisere visse bestemmelser med henblik på at sikre korrekt efterlevelse af reglerne i virksomheder og organisationer, der håndterer persondata. IT-Branchen indgår meget gerne i et tæt samarbejde med myndigheder om at styrke de operationelle vejledningerne til myndigheder, virksomheder og leverandører om, hvordan en god og afbalanceret it-sikkerhed opnås.

- IT-Branchen støtter udvalgenes tilskyndelse til, at afdækningen af Se&Hør-sagen prioriteres. Når der er foretaget en afdækning af sagen vil der være etableret et fyldestgørende grundlag for at gå videre med konkrete overvejelser om nyttevirkningen af eventuel ændret regulering eller andre tiltag. Baseret på den forhåndenværende information samt IT-Branchens drøftelser i medlemskredsen er der ikke tale om et generelt anslag mod IT- eller datasikkerheden i virksomhederne eller tegn på, at IT- eller datasikkerheden i virksomhederne generelt er utilstrækkelig og udgør et problem.

- IT-Branchen støtter som foreslået af udvalgene, at kortlægningen af sikkerhedsproblemer udvides til at omfatte alle områder, hvor der opbevares personfølsomme oplysninger og data. Fokus på it-sikkerhed er nødvendig både hos leverandører, myndigheder og private virksomheder.

- Arbejdsgruppen vedrørende datasikkerhed under Folketingets Retsudvalg planlægger aktivt at inddrage tekniske og juridiske eksperter fra diverse instanser og organisationer. IT-Branchen ønsker i den forbindelse, at der også aktivt inddrages eksperter fra virksomhedssiden, der har praktisk erfaring på området. IT-Branchen deltager meget gerne med vores viden i ekspertpanel mm. i forbindelse med udvalgenes behandling af emnet.

- IT-Branchen støtter op om den konkrete kortlægning af regler og tilsyn. IT-Branchen er dog af den opfattelse, at reglerne på persondataområdet er klare og fyldestgørende, hvorfor arbejdet ikke må udmønte sig i en række administrative byrder for erhvervslivet, som ikke reelt resulterer i bedre databeskyttelse. I den forbindelse er det også vigtigt, at eventuelle nye tiltag ikke unødigt vanskeliggør virksomheders og organisationers evne til at levere god, effektiv og ordentlig kundeservice, eller at samfundets fortsatte digitalisering på nogen måde bliver afsporet.

- IT-Branchen arbejder med udviklingen af en fælles ramme, der kan bruges af leverandører, myndigheder og virksomheder, til at skabe et lettere overblik over hvilket sikkerhedsniveau man ønsker

at være på, samt hvilke afledte anbefalede krav, sikkerhedspolitikker og kontroller man derfor bør efterleve. IT-Branchen vil meget gerne ved et fortræde for udvalgene præsentere arbejdet og dets anvendelsesmuligheder i forhold til at sikre en god balance i IT-sikkerheden i Danmark.

For spørgsmål til ovenstående, samt planlægning vedr. fortræde/præsentation/ekspertdeltagelse ved udvalgsbehandling venligst kontakt:

IT-Branchens IT-Sikkerhedsudvalg, ved chefkonsulent, Bjørn Borre, bjb@itb.dk tlf. 27522524

Vh
Bjørn Borre
IT-Branchen

IT-Branchen
Børsen – 1217 København K
Direkte: +45 7225 5503
Mobil: +45 2752 2524
E-mail: bjb@itb.dk
Web: itb.dk