

Privatlivets fred

- Ikke i Danmark?

Baggrund

Sikkerhed og tillid til it-systemer er af væsentlig betydning for at sikre de effektivitetsgevinster, der ligger i at digitalisere den offentlige forvaltning. Dette indebærer, at borgerne må have sikkerhed for, at der kun indsamles de nødvendige informationer, at disse kun gøres personhenførbare i det omfang det anses for at være nødvendigt, at de oplysninger, som gøres personhenførbare, er sikret på passende vis, og at der kun er adgang til informationerne for de relevante parter.

ITEK og Dansk Industri vurderer, at der de senere år er sket et skred i forhold til, hvilke oplysninger der indsamles, og hvilke der gøres personhenførbare. Der er opstået et bredt politisk ønske, om at overvåge borgerne og registrere deres adfærd i flere sammenhænge. Samtidig sker der i en lang række tilfælde ikke en passende beskyttelse af de oplysninger, der indsamles om borgerne.

Den ekstra overvågning og registrering har gjort, at Danmark i internationale sammenligninger ikke længere er blandt de foregangslande, som respekterer den grundlæggende menneskerettighed: at beskytte privatlivets fred. Ifølge Privacy International¹ var Danmark i 2005 dårligere til at beskytte privatlivets fred end lande som Tyskland, Østrig, Polen, Frankrig og Italien. Danmark ligger i kategori med lande som Israel, Spanien, Argentina og Sverige. Dette skal endog ses i lyset af, at vurderingen er fra 2005, og der er sket mange overvågningstiltag siden da. Disse overvågningstiltag omfatter bl.a. logning af borgernes anvendelse af internet og e-mail i hjemmet og ændringer i retsplejeloven.

Hertil kommer, at den stigende digitale overvågning og registrering ikke har resulteret i, at den myndighed, som skal kontrollere og beskytte vores privatlivs fred, Datatilsynet, er blevet styrket tilsvarende. Tilsynet skal i stedet løfte stadig flere opgaver. Som eksempel på Tilsynets muligheder for at kontrollere Persondatalovens efterlevelse kan fremhæves, at der i perioden 2000-2003 årligt blev gennemført i gennemsnit 70 inspektioner. Da der i dag er anmeldt 3600 dataansvarlige og databehandlere betyder dette, at Datatilsynet kan foretage inspektion hos disse hvert 51. år². Dette må vurderes som kvantitativt utilfredsstillende.

Tilsynet kan heller ikke engagere sig med vejledning i forhold til de parter, der måtte have ønske om det. Der er ikke tilstrækkelige ressourcer eller kompetencer til at deltage i internationalt arbejde udover artikel 29-gruppen. Der er ikke mulighed for overordnet at få hjælp til vurdering af nye teknologier. Endelig er der ingen garanti for, at kvaliteten af de undersøgelser, som Datatilsynet foretager, er tilstrækkeligt grundig. Disse dele påpeges bl.a. i Teknologirådets rapport, som belyser tingenes tilstand i flere europæiske datatilsyn³.

Ved digitaliseringen af den offentlige sektor savnes der en strategi for, hvordan man på den ene side kan forbedre serviceniveauet for borgerne og effektiviteten i den offentlige sektor samtidig med, at man på den anden side bevarer respekten for privatlivets fred og borgernes personhenførbare oplysninger. Den Digitale Taskforce har fokuseret på sikkerhedsimplementering gennem efterlevelse af DS484. Dette styrker ”sikkerheden” i forhold til visse typer trusler (f.eks. i form af at de er tilgængelige og at hackere ikke kan få adgang) men med mindre der samtidig specielt fokuseres på Persondataloven, giver man ikke ”sikkerhed” i betydningen at beskytte privatlivets fred.

¹ [http://www.privacyinternational.org/article.shtml?cmd\[347\]=x-347-545269](http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-545269)

² http://www.folketinget.dk/img20031/udvliblag/lib3/20031_10383/20031_10383.pdf

³ <http://www.eptanetwork.org/EPTA/EPTA-report-ict-and-privacy-in-europe.pdf>

Uden en fælles national strategi og uden centralt udviklede værktøjer er det vanskeligt for indkøbere og udviklere i mindre offentlige enheder – som f.eks. kommuner – at overskue konsekvenserne af de it-systemer til borgerservices, som indkøbes og udvikles i disse år. Og uden en national strategi har man ikke fælles målestok til at vurdere de store nye centrale systemer, der planlægges og udvikles i regi af Den Digitale Taskforce. Hvis kunderne i form af den offentlige sektor i bred forstand ikke stiller krav om disse forhold, har leverandørerne af it-systemer heller ikke nogen mulighed for at tilvejebringe disse løsninger.

Introduktionen af privacy kunne ses som en ekstra mulighed for hvordan man kan forbedre kvaliteten for borgerne samtidig med at borgeren sættes i centrum, når hans data behandles. Der kunne skabes en mulighed for at borgerne kunne kontrollere egne data. Herved kan borgerne dels selv sikre, at data er opdaterede og korrekte, og dels kan borgeren bestemme, hvem der må udveksle hvilke data. Det vil kræve en ny måde at tænke borgerservice på.

Der er blevet gjort opmærksom på disse udfordringer fra mange sider! Først i Metagroups rapport til Videnskabsministeriet om privacy fra marts 2005, hvor det bl.a. hedder: "... it could be valuable to establish a set of architecture principles for privacy, and to include the privacy requirements in the enterprise architecture work currently in progress under the Danish it architecture and software strategy"⁴. Videnskabsministeriets Sikkerhedspanel har rejst sagen og vejledt Ministeriet i forhold til, hvad der burde gøres⁵. Det uafhængige Rådet for IT- og Persondatasikkerhed og Ingeniørforeningen har påpeget den manglende beskyttelse af privatlivets fred i forbindelse med EPJ. Stort set samtlige organisationer i dette land opponeret mod logningsbekendtgørelsen. Flere leverandører har i forbindelse med konkrete projekter præsenteret løsninger, som kunne råde bod på problemerne. Det er vanskeligt at se, at nogle af disse råd, skulle være taget til efterretning i den offentlige sektor.

ITEK og Dansk Industri har indsamlet dette katalog over forskellige brud på privacy og manglende design af privacy i systemer for at synliggøre og dokumentere tingenes tilstand og på denne baggrund rejse en politisk debat om emnet. Indsamlingen er foregået ganske uvidenskabeligt i og med, at vi blot har kigget på Datatilsynets hjemmeside, surfet efter tilfælde omtalt i medierne og spurgt en mindre gruppe medlemmer om deres erfaringer. Der er således ikke tale om et komplet billede af sagens tilstand. Vi har desuden blandt de cases, vi har fundet, afvist en række, som krævede en mere tilbunds gående undersøgelse, end det har været muligt at udarbejde til dette dokument.

I dette katalog vil der blive gennemgået

- Cases som demonstrerer faktiske brud på privatlivets fred i den offentlige sektor
- Planlagte nationale løsninger, som ikke respekterer privatlivets fred
- Politiske tiltag som udvander privatlivets fred

Politiske løsninger

Der skal ikke kun sættes en kritisk dagsorden med dette udspil! Med dette katalog vil ITEK og Dansk Industri gerne pege på forskellige løsningsforslag, som kan dæmme op for problemerne. De mest centrale elementer er:

⁴ <http://videnskabsministeriet.dk/site/forside/publikationer/2006/privacy-enhancing-technologies/Rapportvedrprivacyenhancingtechnologies.pdf>, p. 37

⁵ <http://www.privacyportal.dk/>

1. at der laves en strategi for beskyttelse af privatlivets fred, som baserer sig på designet af og arkitekturen for it-systemerne
2. at denne strategi systematisk fastholdes af et organ i den offentlige sektor
3. at det vurderes om Datatilsynet har de fornødne ressourcer til at opfylde sin opgave.

Der er flere muligheder for at opfylde de tre faktorer. En af mulighederne er at styrke det eksisterende IT-sikkerhedspanel under Videnskabsministeriet således at det dels får et dedikeret sekretariat og dels foruden at rådgive Videnskabsministeriet også høres af og rådgiver Den Digitale Taskforce.

En anden mulighed er at basere strategien på et nyt Informationssikkerhedsråd, der udmærket kan sammensættes som det eksisterende IT-sikkerhedspanel med bred repræsentation fra forbrugerne, rettighedsorganisationerne, industrien, fagbevægelsen, den offentlige sektor og forskningen - meget ala sammensætningen i det nuværende IT-sikkerhedspanel.

Det pågældende organ skal:

- Sikres selvstændighed og have eget sekretariat.
- Have mulighed for at vurdere nye større offentlige IT-projekter for alle ministerielle ressortområder samt kommuner og regioner ud fra tekniske, etiske og juridiske dimensioner - og herunder at disse vurderinger sker i samspil med Datarådet.
- Arbejde for at der laves en overordnet strategi for privacy enabling af digital forvaltning.
- I samarbejde med Den Digitale Taskforce og Videnskabsministeriets møderække om privacy skabes et værktøj, som kan sikre, at værdierne for privatlivets fred, som opstillet i den udmærkede "Lov om behandling af personoplysninger", faktisk implementeres allerede når arkitekturen til nye it-systemer fastlægges. Dette kan gøres ved f.eks. at tage udgangspunkt i ITEK og Dansk Industris vejledning: "God privacy Praksis" eller ved at foretage et Privacy Impact Assessment (PIA), som anbefalet af det canadiske datatilsyn⁶.
- Bidrage til at vurdere om Datatilsynet har de kvantitative og kvalitative ressourcer, som er nødvendige for at foretage et tilfredsstillende tilsyn af danske it-løsningers efterlevelse af "Lov om behandling af personoplysninger".
- Bidrage til at sikre en debat om privacy således at der fra politisk side udvises mådehold med at anvende nye digitale muligheder for overvågning og registrering af borgerne og ikke vedtages lovgivning, som tilsidesætter hensynene i "Lov om behandling af personoplysninger".
- Udarbejde vejledninger til borgere og virksomheder om, hvordan de kan beskytte sig, når de står overfor en it-løsning, som ikke tilbyder at beskytte deres privatliv.
- Arbejde for at der sker en styrkelse af forskningen og modningen af privacy fremmende teknologier (Privacy Enhancing Technologies, PET). Herunder bør der iværksættes konkrete og ambitiøse pilotprojekter med henblik på at etablere læring.
- Arbejde for at der sker en koordineret indsats i forhold til internationale organer, som for eksempel EU-kommissionens indsats omkring privacy og RFID og OECDs privacyarbejde i WPISP, for at fremme retten til privatlivets fred.

⁶ http://www.tbs-sct.gc.ca/pubs_pol/ciopubs/pia-pefr/siglist_e.asp

Cases som demonstrerer faktiske brud på privatlivets fred i den offentlige sektor

STATEN

1. Adgangskontrol i Ligestillingsafdelingen hos Socialministeriet

Adgangskontrollen til et ældre system, der var overført fra Boligministeriet til Socialministeriet, var blevet krænket og havde givet adgang til personhenførbare oplysninger. På trods af at hullet var kendt, tog det næsten et år at få udbedret sagen.

(<http://www.datatilsynet.dk/publikationer/aarsrapport03/07.htm#06>)

2. Behandling af meget følsomme oplysninger uden tilstrækkelig datasikkerhed

Datatilsynet fandt det særdeles kritisabelt og foretog indberetning til Socialministeriet, da det var konstateret, at behandlingen af følsomme personoplysninger i et projekt på en række punkter ikke var sket under iagttagelse af persondataloven. Der var bl.a. sket registrering, uden at kravene om logning var efterlevet, der var ikke fastsat af uddybende sikkerhedsregler, og der var anvendt pc-arbejdspladser uden for den dataansvarliges lokaler uden, at der var fastsat særlige retningslinier herfor.

(<http://www.datatilsynet.dk/attachments/20052493650/brev%20af%202005-03-18%20projekt%20janus.pdf>)

3. Bibliotekssagen

Datatilsynet udtaler, at de undtagelsesvis kan acceptere, at Biblioteksstyrelsen og bibliotekerne foreløbig i en periode på 5 år fortsætter med at sende elektroniske reserverings- og kvitteringsmeddelelser, der indeholder titel og forfatter på det reservede materiale, i ikke-krypteret form til de brugere, der ønsker at benytte elektronisk kommunikation med biblioteksvæsenet.

(<http://www.datatilsynet.dk/publikationer/aarsrapport05/kap04.htm>)

4. Overvågning af offentligt ansattes kommunikation på arbejdspladsen

Den offentlige sektor arbejder med stadigt mere detaljeret overvågning af alle ansatte. Offentligt ansatte ved godt, at det kan være farligt at arbejde med skriftlig kommunikation, men samtidig gør den offentlige sektor ikke meget for at beskytte de ansattes private kommunikation fra arbejdspladsen. Hertil kommer, at der er flere sager, hvor de ansattes ytringsfrihed er sat under pres.

(<http://politiken.dk/VisArtikel.iasp?PageID=283788>,
<http://www.ugebreveta4.dk/view.asp?ID=2951>)

5. Skattevæsenet rammer sæddonorere

Skattevæsenet kræver at sædbanken opgiver navnet på donorerne, så de kan betale skat af de kr. 300,-, de modtager for at donere. Videregivelse af donorerens identitet i form af navn og adresse til skattemyndighederne kan ske som følge af regler i skattekontrolloven. Disse regler indebærer også, at sædbankerne kan registrere oplysninger om donors navn, adresse og personnummer uden samtykke hertil fra donoren. Kravet om anonymitet, som findes i lov om kunstig befrugtning, gælder alene for forholdet mellem donor, modtager, dennes ægtefælle/samlever og eventuelle børn, men ikke i forhold til skattemyndighederne.

Opgivelsen af navnet er dog teknisk set ikke nødvendigt for at opkræve skat af beløbet. I dette tilfælde risikerer man, at kränkelsen af donorens privacy betyder, at donoren ikke længere vil donere, fordi han er identificeret overfor skattevæsenet i en vis periode.

(<http://borsen.dk/nyhed/92930/>,

<http://www.datatilsynet.dk/attachments/200642111156/Brev%20af%202006-07-04%20Vedr.%20saedbank%20A.pdf>,
<http://www.datatilsynet.dk/attachments/200642111156/Brev%20af%202006-07-04%20SKAT%20anonymiseret.pdf>,
<http://www.datatilsynet.dk/attachments/200642111156/Brev%20af%202006-07-04%20vedr.%20saedbank%20B.pdf>)

POLITIET

6. Fejl i Rigspolitiets indberetninger af uønskede udlændinge til Schengen-informationssystemet

En undersøgelse af de 443 danske indberetninger til Schengen-informationssystemet vedrørende uønskede udlændinge viste, at der er sket fejlagtig indberetning i 25 tilfælde.

(http://www.datatilsynet.dk/include/show.article.asp?cat_id=1&art_id=710&sub_url=/Vaerd_at_vid_e/nyheder/arkiv.asp)

7. Politiet sender fortrolige oplysninger til teleselskaber

Teleselskaberne får hele dommerkendelser, smækfyldt med følsomme oplysninger om strafbare forhold, hver gang politiet begærer en telefon aflyttet. Teleselskaberne må selv finde ud af, hvordan de håndterer de følsomme oplysninger om disse mistænkte, der også har en rolle som teleselskabernes egne kunder.

(<http://www.computerworld.dk/art/17097?cid=4&q=personoplysninger&sm=search&a=cid&i=4&o=44&pos=5>)

8. Kalundborg Politi indberettet til Rigspolitichefen for brud på persondataloven

Kalundborg Politi har i flere år anvendt et internt register med følsomme oplysninger, som medarbejderne frit kunne gå ind i.

(<http://www.computerworld.dk/art/14254?cid=4&q=personoplysninger&sm=search&a=cid&i=4&o=57&pos=18>

http://www.datatilsynet.dk/include/show.article.asp?cat_id=1&art_id=558&sub_url=/Vaerd_at_vid_e/nyheder/arkiv.asp)

9. Opfyldelse af logningskrav

Et problem, som Datatilsynet stødte på i 2003, er offentlige myndigheders manglende opfyldelse af sikkerhedsbekendtgørelsens regler om logning af brug af fortrolige personoplysninger eller sletning af oplysningerne efter en vis kortere periode. Der henvises igen til politiet som eksempel.

(<http://www.datatilsynet.dk/publikationer/aarsrapport03/08.htm#04>)

KOMMUNER

10. Kommune pålagde medarbejder at bruge sin personlige "fælles pinkode"

Kommunens anvendelse af en medarbejders "Fælles Pinkode" – som tillige anvendes af medarbejderen som personlig adgangskode i ikke-arbejdsrelaterede sammenhænge – som adgangskode til kommunens systemer, var ikke i overensstemmelse med persondataloven.

(<http://www.datatilsynet.dk/attachments/2005630122154/Brev%20af%202005-09-26%20til%20M%20Kommune.pdf>)

11. Oplysninger i kommunal afskedigelsessag tilgængelige for alle medarbejdere i afdelingen

Datatilsynet fandt ikke, at en kommune havde sandsynliggjort, at de 46 medarbejdere i afdelingen, som havde adgang til det drev, hvorpå oplysningerne om afskedigelsessagen var lagret, havde haft et sagligt behov for at have adgang til oplysningerne om afskedigelsessagen.

(<http://www.datatilsynet.dk/attachments/20052493650/Brev%20af%202004-08-12%20til%20Udeladt%20modtager.pdf>)

12. Personfølsomme oplysninger sendt pr mail

En mail indeholdende personfølsomme oplysninger om en patient blev sendt fra psykiatrisk hospital i Århus til en speciallæge, uden at der var anvendt kryptering eller digital signatur. En virus på speciallægens computer bevirkede, at mailen blev sendt til en række uvedkommende modtagere.

(<http://www.datatilsynet.dk/publikationer/aarsrapport03/07.htm#03>)

13. Kommunes register i strid med persondataloven

I forbindelse med afholdelse af en inspektion i Bogense kommune konstaterede Datatilsynet, at kommunen igennem længere tid havde ført to systemer, uden at reglerne om anmeldelse til Datatilsynet og sikkerhedsreglerne vedrørende logging havde været overholdt.

(<http://www.datatilsynet.dk/attachments/20052493650/Brev%20af%202001-05-22%20til%20Kommunalbestyrelsen%20i%20A%20Kommune.pdf>,

http://www.datatilsynet.dk/include/show.article.asp?cat_id=1&art_id=517&sub_url=/Vaerd_at_vid_e/nyheder/arkiv.asp)

14. Ubeskyttede PDA med personhenførbare oplysninger

Ved hjemmeplejen i en stor dansk kommune bruger de ansatte en PDA med mobiltelefon, således at hjemmehjælperne kan indrapportere, hvor langt de er nået med deres arbejde, og dermed hvem de har besøgt. Formålet med det er, at man fra centralt hold kan rykke om på turene, hvis arbejdsbelastningen er skæv. På PDA'en ligger der information om alle i distriktet, der modtager hjemmehjælp tillige nogle informationer om helbred og medicin på "kunderne". Hjemmehjælperen har dermed relevant viden om "kunden", der besøges.

PDA'en er imidlertid ikke sikret: den kan tændes uden angivelse af password, og applikationen med personhenførbare data kan åbnes uden yderligere sikring. Hvis PDA'en tabes, stjæles eller tilgås uautoriseret af f.eks. et familiemedlem kan man umiddelbart se de fortrolige informationer.

Kommunen burde have sikret PDA'en med sikker logon og kryptering af lagrede data, og ved at der kun fremsendes data på næste aktuelle "kunde", så en eventuel misbrugssituation kunne minimeres. Den kommunale indkøber bør støttes i dette.

(anonym case)

15. Libanesere tjekkes for socialt bedrageri – eksempel på function creep

Under konflikten i Libanon blev libanesere bosat i Danmark men på ferie i Libanon hjulpet til hjemrejse af den danske stat. Efterfølgende er kommuner blevet bedt om at samkøre passagerlisterne med lister over kontanthjælpsmodtagere for at undersøge, om nogle af libaneserne modtog kontanthjælp uden at stå til rådighed for arbejdsmarkedet. Argumentet var, at den kontrol kunne man ligeså godt gennemføre, når man har registreret oplysningerne. Der er tale om function creep, for det er ikke fast rutine, at alle udlandsrejsende skal registreres og kontrolleres for socialt bedrageri.

(http://www.datatilsynet.dk/include/show.article.asp?cat_id=1&art_id=750&sub_url=%2FVaerd%5Fat%5Fvide%2Fnyheder%2Findhold%2Easp)

16. Personhenførbare data om medarbejdere flyder på plejehjem

En svensk medarbejder er ansat på et plejehjem som ufaglært, hvilket er i strid med reglerne, da kravet er, at man skal være faglært. Kollegerne er utilfredse med denne afvigelse fra kravet. En "anonym" kollega sender derfor et brev til personaleafdelingen og anfører heri kollegaens svenske personnummer, som alle medarbejdere har adgang til fordi vagtlistor og journaler ligger frit fremme uden opsyn (primært skrevne lister). Kollegaen anmelder sagen til svensk politi, der dog ikke kan gøre noget, fordi den pågældende svenske medarbejder er ansat i DK.

Lister med personhenførbare informationer om ansatte bør ikke være tilgængelige for alle ansatte i en virksomhed.

(anonym case)

17. Borgerrepræsentationens medlemmer uddeler brugernavn og adgangskode til uvedkommende

En række af borgerrepræsentations medlemmer delte deres adgangskode til den bærbare computer, de havde fået udleveret til at foretage arbejde fra hjemmet, med deres familie og andre. Det betyder, at disse brugere kan få adgang til kommunens informationer og herunder til personhenførbare oplysninger om kommunens borgere.

(<http://www.bt.dk/article/20040819/NYHEDER/108190328/1044>)

18. Kommuners udlevering af skatteoplysninger

Det lykkedes en journalist at få udleveret en række oplysninger om sine kolleger ved at ringe til en kommune og alene opgive de pågældende personers personnumre. Kommunerne havde udleveret data uden at sikre sig behørigt for, at den der ringede og kunne oplyse personnummeret, faktisk var den person, som ejede personnummeret.

(<http://www.datatilsynet.dk/publikationer/aarsrapport04/kap04.htm>)

19. Login på Hinnerup Bibliotek

Hinnerup Bibliotek anvendte en uhensigtsmæssig login. Biblioteket fjernede login-felterne efter henvendelse fra Datatilsynet.

(Datatilsynet)

20. Misbrug af persondata i Holstebro Kommune

Oplysninger fra kommunens R75 register blev videregivet til det lokale dagblad. Kommunen undersøgte sagen bl.a. ved hjælp af loggen, og det blev bl.a. afdækket, at en medarbejder havde søgt i data uden at have haft en sagsbehandlingsmæssig eller faglig interesse i indholdet. En anden medarbejder havde opbevaret sin adgangskode i sin kalender på kontoret i strid med kommunens retningslinier.

(http://www.datatilsynet.dk/include/show.article.asp?cat_id=1&art_id=465&sub_url=/Vaerd_at_vid_e/nyheder/arkiv.asp)

(http://www.datatilsynet.dk/include/show.article.asp?cat_id=1&art_id=531&sub_url=/Vaerd_at_vid_e/nyheder/arkiv.asp)

21. Sikkerhedsbrist i Helsingør Kommunes trådløse net

Helsingør Kommunes trådløse netværk opfyldte ikke opfylder de sikkerhedskrav, som Datatilsynet stiller til trådløse netværk, hvori der transporteres følsomme personoplysninger.

(http://www.datatilsynet.dk/include/show.article.asp?cat_id=1&art_id=613&sub_url=/Vaerd_at_vid_e/nyheder/arkiv.asp)

22. Folkeskoler overtræder persondatalov

At det kræver tilladelse at offentliggøre en medarbejders private telefonnummer på nettet kommer helt bag på danske folkeskoler. Skolernes hjemmesider overtræder i mange tilfælde loven, viser en stikprøveundersøgelse.

(<http://www.computerworld.dk/art/18220?cid=4&q=personoplysninger&sm=search&a=cid&i=4&o=41&pos=2>)

23. Folkekirken

Folkekirken skal følge almindelige forvaltningsretlige regler og persondataloven inklusive de bestemmelser i den, der gælder for offentlig forvaltning. Imidlertid findes der flere eksempler på kirker, som ikke formår at håndtere almindelig it-sikkerhed, videresendelse af mail, brevhemmelighed vedr. oplysninger i menighedsrådsregi etc, da dette er overladt til det enkelte menighedsråd.

Hidtil har mange menighedsråd sendt data, der var fortrolige efter persondatalovens § 7, frem og tilbage over det åbne net. I 2007 – hvilket må betegnes som ret sent – rulles der to løsninger ud: det digitale skrivebord og digital signatur med virksomhedscertifikat. Når dette er taget i anvendelse, resterer der kun nedenstående:

1) Bærbare PC'er og hjemmearbejdspladser (der er stort set ikke andet!), bør sikres i henhold til sikkerhedsbekendtgørelsen jf persondatalovens § 41, stk.3. gennem kryptering af harddiskene.

2) Trådløse netværk skal sikres mod indtrængen udefra.

3) Harddiske, der skrottes, slettes ikke efter bestemmelserne i sikkerhedsbekendtgørelsen.

(anonym case)

KOMMUNERS DATA PÅ INTERNET

24. Generelt om kommuners offentliggørelse af personhenførbare data på internettet

En række sager har vedrørt det forhold, at kommuner er kommet til at offentliggøre personhenførbare data om kommunens borgere på internettet. Årsagen er, at kommunerne som led i offentlighed i forvaltningen har lagt dagsordener og bilag fra møder på internettet uden at slette de personførbare data disse måtte indeholde. En række af disse sager kan henføres til kommunernes anvendelse af KMD's PolWeb. Datatilsynet er i gang med at undersøge, om der er behov for at foretage en egentlig analyse af dette program. Søgemaskiner som Google fanger oplysningerne, hvilket komplicerer problemet yderligere, fordi det derefter er det næsten umuligt at få dem slettet igen fra samtlige søgemaskiner.

25. Overtrædelse af persondataloven i kommuner

Datatilsynets inspektioner afslørede overtrædelser af persondataloven i flere kommuner i Nordjylland. Et problem, som tilsynet jævnligt er stødt på, er offentlige myndigheders manglende opfyldelse af sikkerhedsbekendtgørelsens regler om logning af brug af personoplysninger eller sletning af oplysningerne efter en vis kortere periode. De kommuner, som det stod særlig slemt til i var Brovst, Sejlflod og Fjerritslev.

([http://www.datatilsynet.dk/include/show.article.asp?cat_id=1&art_id=575&sub_url=/Vaerd at vide/nyheder/arkiv.asp](http://www.datatilsynet.dk/include/show.article.asp?cat_id=1&art_id=575&sub_url=/Vaerd+at+vide/nyheder/arkiv.asp)

<http://www.datatilsynet.dk/publikationer/aarsrapport02/06.htm#04>)

26. Sundsøre kommune lægger personhenførbare oplysninger på nettet

I forbindelse med offentliggørelser af dagsordener fra møder, hvor der blev behandlet sager vedrørende kommunens borgere, var Sundsøre kommune kommet til at lægge oplysninger om borgerne, der var behandlet på møderne og derfor omtalt i mødets bilag, på nettet.

(DR, TV-avisen 21:00, 19. august 2004,

<http://www.datatilsynet.dk/publikationer/aarsrapport04/kap04.htm>)

27. Gladsaxe kommune lægger personhenførbare oplysninger på nettet (x3)

Gladsaxe kommune var kommet til ved en administrativ fejl at lægge personhenførbare oplysninger på nettet.

(<http://www.datatilsynet.dk/publikationer/aarsrapport05/kap04.htm>)

Som et kuriosum kan det tilføjes at en tilsvarende sag mod samme kommune blev rejst både primo og ultimo 2006.

28. Præstø kommune lægger personhenførbare oplysninger på nettet

Præstø kommune placerede ved en fejl personhenførbare oplysninger om asylansøgere på sin hjemmeside. Sagen blev efterfølgende behandlet af Datatilsynet, som fandt sagen meget beklagelig. (Politiken, 18/10 2006)

29. Trundholm kommune lægger personhenførbare oplysninger på nettet

Trundholm kommune var kommet til ved en administrativ fejl at lægge personhenførbare oplysninger på nettet.

(Politiken, 18/10 2006)

Planlagte nationale løsninger, som ikke respekterer privatlivets fred

GENERELLE OVERVEJELSER OM ADGANGSKONTROL

30. Sundhedsportalen/Borgerportalen/Virksomhedsportalen

Tanken om een indgang til det offentlige er en god ide for så vidt angår muligheden for at få overblik over services og information.

Men fordi man koncentrerer login med en og samme nøgle til alle dele af den offentlige forvaltning og kobler disse i "Min Side" skaber man såkaldt "single point of trust failure", for de brugere, der ikke har trust til den offentlige administration af data.

Hertil kommer at der også er risiko for at skabe en central registersamkøring af borgernes data når disse samles eet sted for borgeren.

De to væsentlige pointer på dette område er at der savnes en national strategi, som sammenfatter to arkitekturkrav:

På den ene side de forhold, der skal beskytte borgerne ved at lade dem give autorisation til hvem i den offentlige forvaltning, der på tværs af sagsområder må tilgå deres data – selvfølgelig med behørig autentifikation og logning af de myndigheder og sagsbehandlere, som får adgang. Det centrale element er her brugerbestemt rollebaseret adgangskontrol frem for linieorienteret adgangskontrol. Grundlæggende skal det sikres, at der ikke indsamles flere oplysninger end nødvendigt, for at sikre at en konkret sagsbehandling kan finde sted.

På den anden side skal det vurderes, om man ikke kan arbejde med en identitetsmodel med flere lag, så grunddata pseudonymiseres, og kun de medarbejdere, som rent faktisk skal kunne identificere borgeren, får adgang hertil. Herunder ideelt set at det vurderes, om eller hvornår det er nødvendigt at identificere borgerne for at behandle deres data. Identifikationskontrollen af borgerne bør gradbøjes efter formålet. Der mangler således også en strategi for, hvornår det må anses for at være nødvendigt at indsamle hvilke oplysninger. Hvilke personhenførbare oplysninger er f.eks. nødvendige for at bestille et nyt pas eller for at bestille en rottefænger? Det to centrale elementer er her mulig pseudonymisering frem for identifikation og formålsspecifikke identiteter frem for generelle identiteter.

Disse overvejelser går igen i flere af de øvrige cases i dette afsnit.

(anonyme cases)

31. Borgerservicecentre har for bred adgang til personhenførbare oplysninger

Der har været behov for at erindre om de skærpede regler for behandling af persondata i kvikskranker mm. hvor kommunalt personale har adgang til et unødvendigt bredt spektrum af information om den enkelte borger. Problemet er overordnet, at de fleste adgange afspejler linieorganisationen og ikke de specifikke roller og relationer for den enkelte medarbejder. Hvis der er brug for tværgående rettigheder, som f.eks. til en kvikskrankemedarbejder, er man nødt til at misbruge/omgå denne struktur (eller med andre ord: give for mange rettigheder). Hertil kommer, at der er begrænset kontrol af den indre infoudveksling mellem forvaltningerne i en kommune.

(<http://www.privacyforum.dk/?p=24>)

NYERE TEKNOLOGIER SOM BIOMETRI OG RFID

32. Biblioteker

Indførelsen af RFID på biblioteker betyder, at de indbyggede RFID-chip på bøgerne kan bruges til at spore borgerne på basis heraf. F.eks. kan man følge borgerne rundt i storcentre etc. Desuden kan man ved at læse chippen, i de tilfælde hvor man har adgang til bibliotekets database over bøger,

finde ud af hvilke bøger borgerne har på sig – uagtet at disse måske handler om politik, religion, sygdomme eller seksualitet. Problemet kan teknisk løses ved enten midlertidig at slå RFID-chippen fra uden for biblioteker - eller endnu bedre at giver borgeren en midlertidig nøgle til de bøger, han har ansvaret for. Samlet løsning for sikring af bibliotekerne med betydelige serviceforbedringsmuligheder er udviklet og præsenteret for Biblioteksforeningen og Biblioteksstyrelsen. Grundet manglende ressourcer er projektet afvist.
(anonym case)

33. Biometrisk pas med RFID chip

Danmark har været en af fortalere for de biometriske pas kombineret med RFID. De nye pas indeholder for tiden alene et elektronisk pasfoto af passets ejer. Et sådant lagret foto er ikke i klassisk forstand biometrisk data. Men fotoet kan tilgås kontaktløst med en RFID-læser. Rigspolitiet fastholder - uden at forholde sig til den dette forhold - alene at passet er sværere at kopiere, hvad der også er korrekt. Men kopiering er kun eet element i sikkerhed. Et andet vigtigt element er sikre, at uvedkommende ikke via RFID chippen kontaktløst kan kopiere oplysninger fra passet og muliggøre f.eks. ægte pas med digitale data fra et andet pas indlagt. Hertil kommer en række eksperter frygt for at udviklingen i retning af pas med mere biometri er starten på en egentlig national database, hvor borgernes biometriske data er registreret. Overordnet skal man være meget forsigtig med at indføre brugen af biometriske nøgler fordi de kan forfalskes. Et minimumskrav er, at de skal kunne tilbageføres uden at blokere for, at borgeren kan få nye nøgler f.eks. ved såkaldt on-card match.

<http://tekno.dk/subpage.php3?article=1114&toppic=kategori6&language=dk>,
http://www.priway.com/docs/idworld_passport_engberg20061129.pdf

DIGITAL SIGNATUR

34. Sikkerhed ved OCES digital signatur

En bruger kunne kompromittere det sikkerhedsniveau, som er fastlagt i den samlede systemløsning, ved ikke at følge en given instruks. Dette betragtede Datatilsynet som en sikkerhedsbrist ved OCES.
<http://www.datatilsynet.dk/publikationer/aarsrapport04/kap04.htm#4.2>

35. Digital signatur

Digital Signatur er lavet med det udgangspunkt at kontrollen altid er centraliseret i en CA og implementerer dermed overvågning af borgerens aktiviteter uden nogen form for indbygget sikkerhed for borgeren. Udgangspunktet er dermed alene at den offentlige forvaltning kan være sikker på, hvem borgeren er, frem for at sikre borgernes informationer. Dette kan bestemt også være nyttigt i en lang række tilfælde med det eksisterende sikkerhedsparadigme, hvor der er behov for at identificere borgeren entydigt, for at give ham adgang til egne informationer eller offentlige services. Den digitale signatur er dermed et godt og vigtigt bidrag til sikkerhed i forbindelse med digital forvaltning.

Men signaturen kunne have været mere nuanceret implementeret. Det kunne imidlertid have været hensigtsmæssigt dersom Digital Signatur blev suppleret med en række sikkerhedshensyn til borgerens fordel såsom specifik tilbageførsel af samtykke samt mulighed for at have mange pseudonyme signaturer til brug for adgangskontrol og specifikke formål.
(anonym case)

SUNDHEDSOPLYSNINGER

36. Medicinprofilen og misbrug af sundhedsoplysninger

Medicinprofilen blev besluttet af Folketinget i 2003 gennem en ændring til lov om offentlig sygesikring.

Tanken om at sikre muligheden for at borgeren og lægen kan tilgå alle medicintransaktioner er glimrende. Ikke mindst fordi det medvirker til at færre bliver fejlbehandlet med medicin. Profilen opdateres for hver enkelt borger af apotekerne.

Det er imidlertid tvunget for alle borgere, at de identificeres, og at deres medicinforbrug skal registreres i profilen.

Hertil kommer, at der er adgang for alle landets læger til at kigge i profilen. Dette er allerede blevet misbrugt af forskellige læger.

Hertil kommer, at man kan give samtykke til at en meget bredere kreds kan få adgang til oplysningerne: apotekspersonale og hjemmeplejen og desuden overvejes det at give adgang for tandlæger og deres personale.

Datatilsynet har siden starten være ganske kritisk overfor medicinprofilen og det er ifølge forskellige kilder ganske tvivlsomt, om det ligger inden for det EU-direktiv, som Lov om behandling af personoplysninger bygger på.

Man kunne sagtens have gennemført en række hensigtsmæssige services i tilknytning til medicinprofilen uden at identifikation og anvendelse af personhenførbare oplysninger havde været nødvendigt. F.eks. kunne man have anvendt pseudonymer og i konkrete sammenhænge givet adgang via certifikater.

(<http://www.medicinprofilen.dk/>, Artikel i WA den 10.11.2006, <http://www.dagensmedicin.dk/opinion/opinion/article/medicinprofil-pa-glidebane/?encryptionKey=Usu37jdSJ7sS888s4958Fj&cHash=9cc60d0331>, <http://www.dagensmedicin.dk/nyheder/nyhed/article/politikere-vil-aendre-epj-lov/?encryptionKey=Usu37jdSJ7sS888s4958Fj&cHash=f7c8c45c19>)

37. Receptserveren

Receptserveren er tænkt som et supplement til Medicinprofilen. På receptserveren skal lægerne placere alle de recepter de udsteder. På den måde skal man fra centralt hold kunne sammenligne mellem, hvad lægen har registreret på receptserveren, og hvad apotekerne har udleveret og registreret på medicinprofilen.

Samtidig åbner profilen op for, at man selv kan vælge det apotek, man vil til at få udleveret sin medicin, fordi apoteket altid kan slå recepten op på en central server. Dette giver borgerne større fleksibilitet.

Der bliver obligatorisk for alle danskere at få registreret deres receptpligtige medicin.

Den kommunale hjemmesygepleje får adgang til oplysningerne.

Igen kunne man sagtens have lavet denne service uden at identificere borgerne.

(<http://www.dagensmedicin.dk/nyheder/nyhed/article/receptserver-vil-gore-fejl-tydeligere/>)

38. e-journal

e-journalen indeholder sygehusenes beskrivelser af patienternes behandling på sygehusene.

Amtsrådsforeningens e-journal-projekt indebærer, at der gives mulighed for, at et meget stort antal personer – i første omgang alle landets 3.500 privatpraktiserende læger via en online adgang – har adgang til oplysninger om alle borgere, der på et eller andet tidspunkt har været i kontakt med et offentligt sygehus. Datatilsynet fandt, at dette var en alt for bred adgang til oplysningerne og derfor skal e-journal begrænses således, at det kun er læger, der behandler en konkret patient, der kan få adgang til oplysningerne. Man kunne sagtens lave løsningen, så kun patienten selv eller en som patienten har delegeret ansvaret til, kan etablere adgang for nye læger til patientens journal.

http://www.datatilsynet.dk/include/show.article.asp?cat_id=1&art_id=742&sub_url=/Vaerd+at+vid+e/nyheder/arkiv.asp
http://www.datatilsynet.dk/include/show.article.asp?cat_id=1&art_id=756&sub_url=%2FVaerd%5Fat%5Fvide%2Fnyheder%2Findhold%2Easp
<http://www.dagensmedicin.dk/nyheder/nyhed/article/oget-kontrol-skal-sikre-e-journal/?encryptionKey=Usu37jdSJ7sS888s4958Fj&cHash=f7c8c45c19>

39. Elektroniske patientdata (EPJ)

Den nye lov om EPJ-adgang afspejler en holdning om, at den differentierede adgangs kontrol skal udføres manuelt og på tro-og-love (og kontrolleres med logning) lige som vi har set det med medicinprofilen og receptserveren. Der har ikke været forståelse for, hvilke krav der skal stilles til systemernes arkitektur for at beskytte patientens persondata.

Oprindeligt blev der fremsat en samlet pakke med ændring af diverse elementer i sundhedsloven m.v. (<http://www.folketinget.dk/?/Samling/20061/lovforslag/L50/index.htm>). Denne lov blev opdelt i L50A, som nu er vedtaget (og som omhandler medicinprofilen m.v.) og L50B, som endnu er under behandling og indeholder bestemmelser for EPJ (<http://www.privacyforum.dk/?p=22>). Fokus har været på at få styrke den semantiske integration, men man har næsten fuldstændigt ignoreret sikkerhedsproblemstillingerne, hvilket har medført kraftig modstand mod og manglende effektivisering af EPJ. Det som skiller vandene er fortsat, at der er en meget bred adgang til EPJ for en meget bred kreds i sundhedssektoren. Der er ikke tænkt i klassificering af data eller rollebestemt adgang til data, og der må være en stram logning af hvem der tilgår data.

(I øvrigt er denne sag et godt eksempel på at it-leverandørerne står frustrerede tilbage. IT-teknisk kan man levere, hvad der er behov for, men der mangler overordnede rammer at bygge udviklingen på.)

<http://www.dagensmedicin.dk/nyheder/nyhed/article/politikere-vil-aendre-epj-lov/?encryptionKey=Usu37jdSJ7sS888s4958Fj&cHash=f7c8c45c19>,
<http://ing.dk/apps/pbcs.dll/article?AID=2007101260029&NL=1&Category=IT>,
<http://www.version2.dk/artikel/1174?rss>)

ANDET

40. "Nem"-konto

NemKonto har til formål at sikre, at det offentlige kan reducere sine transaktionsomkostninger, når der skal overføres penge til borgerne. Dette sker ved, at alle borgere som minimum skal have oprettet en konto i et pengeinstitut, og at én af disse gøres til borgerens NemKonto, hvortil det offentlige kan overføre alle midler.

Ved at "kollapse" alle økonomiske mellemværender med det offentlige til en enkelt konto, ser man stort på, at økonomiske transaktioner med borgere meget vel kan opfattes som følsomme informationer. NemKontoen betyder, at pengeinstitutterne kan få et samlet overblik over borgerens relation med det offentlige og hvilke serviceområder, der interagerer med borgerne.

Datatilsynet har udtalt sig om NemKonto og ikke fundet anledning til kritik. Tilsynet fremhæver dog, at det er en forudsætning, at NemKonto ajourføres, og at den enkelte sagsbehandler ikke får adgang til oplysninger om konkrete pengeinstitutkonti, der er indeholdt i NemKonto registeret. Datatilsynet har ikke forholdt sig til, at pengeinstitutterne kan skabe sig et samlet billede af borgerens samlede økonomiske relation med det offentlige.

(www.nemkonto.dk, <http://www.datatilsynet.dk/publikationer/aarsrapport03/04.htm#02>)

Man kan yderligere tilføje, at det må være en forudsætning, at de konkrete sagsbehandlere ikke får adgang til at danne sig et samlet billede af overførsler til borgeren ved at kunne slå op på NemKontoen – med mindre dette er sagligt begrundet.

Yderligere kan det tilføjes, at en tilsvarende service sagtens kunne være etableret gennem anvendelse af pseudonymer – en egentlig identifikation af borgeren er unødvendigt.

Politiske tiltag som udvander privatlivets fred

41. Lovgivning på sundhedsområdet

Som det fremgår ovenfor er der lavet og planlagt en række ændringer af lovgivningen, der muliggør medicinprofilen, receptserveren, e-journal og EPJ. Datatilsynet har været skeptisk overfor disse ændringer. Idet der mangler den fornødne proportionalitet mellem indsamling af oplysninger og opfyldelsen af de formål, der var fastsat i lovforslagene. Sammenfattende gav forslagene således indtryk af, at der ville blive indsamlet en stor mængde af data, som man kun i visse tilfælde, og kun visse grupper af ansatte ville have brug for, for at give patienterne den rette behandling. Det er ligeledes tvivlsomt, om lovgivningen er i overensstemmelse med EU-direktivet. Dette kan betyde, at såvel lovgivning som systemer på sundhedsområdet senere skal laves om.

42. Lovgivning om offentlighed i retsplejen

Datatilsynet fandt, at hensynet til offentlighed i retsplejen meget nøje måtte afvejes i forhold til hensynet til beskyttelsen af følsomme personoplysninger. Forslaget havde efter tilsynets opfattelse databeskyttelsesretlige konsekvenser, der af den enkelte borger ville kunne opleves som en forringelse af beskyttelsesniveauet og en krænkelse af den personlige integritet, f.eks. ved at følsomme oplysninger ville blive videregivet i skriftlig form til uvedkommende personer. Datatilsynet pegede i den forbindelse også på, at de begrænsninger i og undtagelser til aktindsigt, der blev lagt op til i forslaget, havde undtagelsens karakter og i vidt omfang beroede på en konkret vurdering i det enkelte tilfælde.

<http://www.datatilsynet.dk/publikationer/aarsrapport03/04.htm#03>

43. Lovgivning om børneattester

Efter Datatilsynets opfattelse gav det anledning til alvorlige overvejelser i forhold til principperne i § 5 om saglighed, rimelighed og proportionalitet at indføre en pligt til at indhente børneattester på en meget omfattende kreds af personer, uden at der i det enkelte tilfælde skal foretages en konkret vurdering af nødvendigheden heraf. Ud fra hensynet til privatlivets fred og i lyset af databeskyttelsesretlige principper om saglighed og proportionalitet, jf. persondatalovens § 5, fandt Datatilsynet endvidere, at det måtte give anledning til bekymring, at oplysninger om alvorlige strafbare forhold spredtes til et stort antal private organisationer, foreninger mv., hvorved en meget bred kreds af personer i princippet vil få adgang til disse oplysninger. Personkredsen vil ofte være uden praktisk erfaring med den måde, hvorpå fortrolige oplysninger skal behandles.

<http://www.datatilsynet.dk/publikationer/aarsrapport04/kap02.htm#2.7>

44. Planer om udveksling af oplysninger mellem retshåndhævende myndigheder inden for Europa

En række initiativer viser en klar udvikling i retning af øget informationsudveksling og intensiveret samarbejde mellem retshåndhævende myndigheder inden for Europa. Datatilsynet har bl.a. tilkendegivet, at udviklingen hen imod øget informationsudveksling aktualiserer behovet for gennemførelsen af et generelt og opdateret databeskyttelsesretligt instrument på dette område.

<http://www.datatilsynet.dk/attachments/200642111156/Brev%20af%202006-03-17%20til%20Justitsministeriet%20sag%200046.pdf>

<http://www.datatilsynet.dk/attachments/200642111156/Brev%20af%202006-03-17%20til%20Justitsministeriet%20sag%200045.pdf>

45. Overvågningskameraer

Der er fremsat lovforslag om at private virksomheder kan foretage tv-overvågning af de områder, der ligger i deres umiddelbare nærhed under forudsætning af at en række omstændigheder er til stede. Forslaget har til formål at reducere kriminalitet.

Forslaget vil i værste fald kunne bruges til at følge borgernes vej gennem det offentlige rum, hvis tv-overvågningen bliver tilstrækkeligt omfattende. Lovforslagets formuleringer, som er baseret på tv-overvågningsudvalgets betænkning viser dog en god balance i forhold til at respektere privatlivets fred.

Det skal bemærkes, at effekten af overvågning på gader og stræder i forhold til kriminalitet drages i tvivl af flere eksperter. Desuden synes der at være empirisk belæg for at overvågningens formål har det med at skride over tid, således at det oprindelige formål hurtigt suppleres af andre formål.

(Betænkning fra udvalg under JM: <http://www.jm.dk/udskriv.asp?page=document&objno=76503>, <http://www.berlingske.dk/indland/artikel:aid=850222/>, <http://www.jm.dk/wimpdoc.asp?page=document&objno=76975>, <http://www.tekno.dk/pdf/nummer198.pdf>, p. 5)

46. Erhvervsministeriet lovforslag om ransagning hos private efter dokumenter fra deres arbejdsplads

Økonomi- og erhvervsministeriet har foreslået Konkurrenceloven ændret således, at der kan foretages ransagning i ansattes private hjem, hvis der er mistanke om at virksomheden har brudt konkurrenceloven. Forslaget er en indskrænkning af privatlivets fred, og ransagningen hos almindelige ansatte er et for voldsomt indgreb, når strafferammen for overtrædelser af Konkurrencelov ikke giver mulighed for fængsel.

(Børsen, 28. november 2006, Berlingske Tidende, 28. november 2006, Retsudvalget, Alm. del, Bilag 109, <http://www.ft.dk/samling/20061/almdel/REU/Bilag/109/318784.PDF>)

47. Antiterrorpakken i 2001

Den første antiterrorpakke var det indledende grundlag for logningsbekendtgørelsen og ændringer i Teleloven, hvorefter teleselskaberne fik pligt til at opbevare oplysninger om borgernes teletrafik i et år. Desuden betød loven, at der blev lavet en bredere definition af terrorisme og desuden øges antallet af mistænkte. Politiet fik også udvidet adgang til at foretage ransagninger og beslaglæggelser. Datatilsynet udtalte betænkeligheder under henvisning til hensynet til privatlivets fred.

(<http://www.datatilsynet.dk/publikationer/aarsrapport01/02.htm#08>)

48. Logningsbekendtgørelsen

Udmøntelsen af antiterrorloven fra 2001, hvorefter teleselskaberne skal indsamle trafikoplysninger om borgerne. Næsten samtlige danske organisationer udtalte sig imod denne bekendtgørelse, som også var fem år undervejs.

(<http://147.29.40.90/GETDOC/ACCN/B20060098805>, <http://147.29.40.91/GETDOC/ACCN/C20060007460-REGL>)

49. Regeringens handlingsplan for terrorbekæmpelse 2005

Regeringen fremlagde i november 2005 en lang række forslag, der i den kommende periode ville blive fremsat i Folketinget. Disse forslag havde til formål at bekæmpe terror. Men ingen af forslagene tog hensyn til privacy, og der var øjensynligt ikke tænkt i, hvordan der kunne etableres proportionalitet mellem indgrebet og formålet med indgrebet. Blandt eksempler fra forslaget kan fremhæves følgende punkter:

15: "...udbydere af elektroniske kommunikationsnet og -tjenester får pligt til at indrette deres tekniske udstyr på en måde, der gør indgreb i meddelelshemmeligheden muligt..."

16: "...det teknologiske område, hvor politiet ikke har nogen umiddelbar mulighed for at sammenholde brugeroplysninger med det enkelte kommunikationsapparat... elimineres..."

17: "...politiet...skal have mulighed for...at indhente fremadrettede tele- og masteoplysninger..."

18: "...politiet...skal have mulighed for...at indhente historiske tele- og masteroplysninger..."

27: "...undlade underretning til en mistænkt om et gennemført indgreb i meddelelshemmeligheden kan ske på baggrund af hensyn til beskyttelse af fortrolige oplysninger om politiets efterforskningsmetoder..."

28: "...det pålægges udbydere af telenet- og teletjenester at udlevere abonnements oplysninger uden rettens godkendelse..."

29: "...politiet i ganske særlige situationer må foretage scanning af indholdet af telefon samtaler eller anden tilsvarende kommunikation inden for et nærmere angivet område..."

33: "...tilvejebringes mulighed for øget og forbedret tv-overvågning af centrale pladser, væsentlige trafikknudepunkter og andre steder..."

(http://www.stm.dk/publikationer/terrorpakke/terrorbekaempelse_endelig.pdf)

50. Antiterrorpakken i 2006

I den anden generation af antiterrorpakken fik PET og Politiet igen nye beføjelser - herunder ret til at indhente oplysninger fra myndigheder uanset oplysningens karakter, og uden at skulle begrunde, at oplysningen indhentes. Politiet kan desuden fra udbydere af telenet eller -tjenester indhente oplysninger om lokaliseringen af en mobiltelefon ved at scanne områder. Politiet kan bede om dommerkendelser til at skanne en person uanset, hvilket udstyr han bruger (herunder også andres udstyr). Politiet kan også forstyrre eller afbryde radio- eller telekommunikation i et område. Politiet kan bede både offentlige og private om at foretage tv-overvågning.

(Retsplejeloven: <http://147.29.40.90/GETDOC1/ACCN/A20060100129-REGL>, <http://www.datatilsynet.dk/attachments/200642111156/Brev%20af%202006-03-23%20til%20jmt.pdf>)