TEKNOLOGI-RÅDET

Elektroniske spor

rapport fra et forprojekt

Projektledelse i Teknologinævnets sekretariat:

Lars Klüver og Steffen Stripp

TeknologiNævnets rapporter 1995/2

ISBN: 87-89098-94-3
ISSN: 0903-2789

Indholdsfortegnelse

1. Projektbeskrivelse

2. Sammenfatning

3. Elektroniske spor
3.1 Hvad er elektroniske spor
3.2 Udviklingstendenser
3.3 Trussel mod den personlige integritet
3.4 Lov om private registre

4. Eksempler på elektroniske spor
4.1 Betalingssystemer: Hvad har du lavet?
4.1.1 Elektronisk betaling
4.1.2 Betalingskortloven
4.2 Telefonsamtaler: Hvem snakker du med?
4.3 Biblioteket: Hvad læser du?
4.4 Trafikinformatik: Hvor har du været?
4.5 Informationsservice-ydelser:
Hvad har du efterspurgt?

5. Handlemuligheder
5.1 Undgå elektroniske spor
5.2 Regulering af sporene

6. Noter

---

1. Projektbeskrivelse

Projektets ide

I stadig flere dagligdags handlinger indgår edb som en del af den samlede teknologianvendelse. I mange sammenhænge vil der ske behandling af personoplysninger og ofte vil den elektroniske behandling kun kunne fungere, hvis der sker en vis registrering af personoplysninger. Med elektroniske spor tænkes på sådanne enkle og i og for sig helt ufarlige registreringer der dannes, som en "bi-effekt" af en almindelig handling. Elektroniske spor er set som en risiko bl.a. som følge af de store mængder persondata der registreres, muligheden for samkøringer som kan danne personprofiler, uhindret videregivelse til markedsføring i strid med personens ønsker og fordi oplysninger som hører til privatlivets fred kan slippe ud til uvedkommende. Anvendelse af betalingskort (Dankort o.l.), som giver elektroniske spor fra betalinger og indkøb, er reguleret i loven om betalingskort. Elektroniske spor vil med den stigende anvendelse af edb blive mere udbredt.

Projektet skal belyse forskellige elektroniske spor og pege på områder, hvor elektroniske spor kan få udbredelse i fremtiden. Dernæst skal fremlægges forskellige muligheder for at imødegå udbredelse af og risiko ved elektroniske spor. Herunder beskrives EU-direktivets regulering af området.

Formål

Formålet med projektet er at

- skabe overblik over udbredelsen af elektroniske spor
- opstille handlemuligheder
- danne grundlag for evt. yderligere vurderingsindsats på området.

Målgrupper og formidling

Som "forprojekt" er målgruppen TeknologiNævnet. Dernæst informeres Folketingets medlemmer og offentligheden gennem en sammenfatning af projektets resultater.

Fremgangsmåde

Projektet gennemføres som en enkeltmands udredning, hvor der indsamles oplysninger fra skriftlige kilder (litteratur, artikler, registerforskrifter mv) og ved kontakt til institutioner og personer. Forskellige elektroniske spor og regulering heraf beskrives i en række arbejdspapirer.

Der udarbejdes et arbejdspapir om handlemuligheder: hvordan undgås elektroniske spor, regulering af anvendelsen, anonymisering mv.

En foreløbig liste over områder, der vil blive belyst:

- betalingskort, registrering af anvendelsessted
- telefonsamtaler, registrering af kaldte nummer
- telefonsamtaler, overførsel af kaldende nummer
- biblioteker, registrering af boglån
- home shopping, registrering af transaktioner
- on-line søgninger, registrering af opkald
- TV og video on demand, registrering af forbrug
- trafik, registrering af den fysiske færden.

2. Sammenfatning

Med elektroniske spor henvises til registreringer af ikke-følsomme oplysninger i edb-systemer, der anvendes i forbindelse hverdagsaktiviteter, som foretages af mange mennesker og gentages ofte af den enkelte. Edb-systemer der danner disse elektroniske spor er karakteriseret ved at

- registreringen sker automatisk,
- der sker ikke en udvælgelse eller behandling af data i forbindelse med registreringen,
- de registrerede oplysninger anvendes til edb-behandling i umiddelbar forlængelse af aktiviteten og
- indsamlingen af data er kendt af den enkelte.

Det er næppe muligt at afdække alle elektroniske spor og det er givet helt umuligt at forudsige de elektroniske spor der vil opstå i fremtiden. Men i takt med fremkomsten af informationssamfundet vil den enkelte i stigende grad kommunikere elektronisk, og der vil opstå stadig flere elektroniske spor - *med mindre der tages særlige initiativer*.

Der dannes elektroniske spor i både den offentlige og den private sektor. I den offentlige sektor medfører den større offentlighed og registerlovens procedure krav, at elektroniske spor behandles ud fra databeskyttelseshensyn før systemerne tages i anvendelse. I den private sektor er der reel mulighed for at systemer, som har omfattende elektroniske spor, opbygges uden forudgående inddragelse af databeskyttelseshensyn og uden tilstrækkelig regulering. Lov om private registre indeholder rammer for registrering og videregivelse af personlige oplysninger, men kan ikke stå alene i reguleringen af disse systemer. Der vil være behov for sær-regler, som det f.eks. er sket med betalingskortloven.

Personlige integritet

De enkelte elektroniske spor er oftest i sig selv uden risiko for den personlige integritet. Men samles elektroniske spor kan der være mulighed for at tegne en detaljeret personprofil. Elektroniske spor kan misbruges af systemejeren eller af uvedkommende, som skaffer sig uautoriseret adgang til dem. Set fra en samfundsmæssig vinkel kan man spørge om det er fornuftigt at opbygge samfundet så der dannes

meget store mængder elektroniske spor, som det er *teknisk muligt* at finde frem og samkøre.

Det kan konstateres, at der er en generel politisk accepteret målsætning om, at udbredte elektroniske spor udgør en trussel, som bør imødegås. Denne databeskyttelses-politik kan gennemføres på to måder. For det første kan man søge helt at undgå, at der dannes elektroniske spor, og for det andet kan man tilvejebringe en regulering af de elektroniske spor som dannes.

Undgå spor

En oplagt og effektiv måde at imødegå risici for den personlige integritet ved elektroniske spor er helt, at undgå at de dannes. Der findes tekniske muligheder for at edb-systemer af denne type kan udformes så der ikke dannes elektroniske spor.

Idag mangler der fremgangsmåder inden for den private sektor, som kan sikre, at der tages stilling til om systemet behøver at registrere personoplysninger og dermed fremme systemdesign, som ikke indebærer elektroniske spor.

Der lægges op til en hastig udbredelse af trafikinformatik i de kommende år. Indførelse af informations- og kommunikationsteknologi i trafikken åbner mulighed for en registrering af personlige oplysninger i en række sammenhænge: registre med betalingsforhold i.f.m. vej- og parkeringsafgifter, trafikregistrering, trafikinformation, hastighedsovervågning. Udvikling af trafikinformatiksystemerne sætter spørgsmålet om registrering af vores fysiske færden på dagsordenen. Der er behov for initiativer, som fremmer, at trafikinformatikken i mindst mulig omfang fører til elektroniske spor.

Med udbredelse af en lang række informationsservice-ydelser vil der blive behov for betalinger af varer og tjenesteydelser over nettet. Der er udviklet et system så disse betalinger kan gennemføres uden der skabes elektroniske spor. Der bør fra pengeinstitutterne eller politisk hold tages initiativ til at sikre, at denne betalingsform også er tilgængelig herhjemme.

Regulering af spor

I de kommende år vil der utvivlsomt ske en betydelige udbredelse af informationsservice-ydelser, som benyttes fra hjemmets pc. Pc'en kan, når den er udstyret med et modem, kommunikere med udbydernes edb-systemer via telenettet.

Man kan forvente et bredt spektrum af serviceydelser: varekøb, bankforretninger, underholdning, tv/video on demand, elektronisk post, nyheder, informationer, selvbetjening hos offentlige myndigheder m.m. Ved fremkomst af mere omfattende systemer med elektroniske spor vil der være behov for en specifik regulering.

Med udgangspunkt i betalingskortloven kan en sådan regulering omfatte

- en nærmere afgrænsning af hvilke oplysninger der må registreres, f.eks. hvilke oplysninger der opfylder formålet
- en fastlæggelse af hvordan de registrerede oplysninger må anvendes, f.eks. at oplysningerne kun må benyttes til nærmere beskrevne opgaver
- en regulering af videregivelse af oplysningerne, f.eks. at oplysningerne kun må videregives i udtrykkelig beskrevne tilfælde

- et krav om sletning af oplysninger, f.eks. at oplysninger skal slettes efter en bestemt kort tidsperiode.

Såfremt EU-direktivet om databeskyttelse vedtages vil det indre marked blive en realitet for personoplysninger. Der må peges på vigtigheden af at det generelle direktiv udfyldes med en specifik regulering for relevante sektorer. Det kan ske ved at databeskyttelses-regulering indarbejdes i direktiver for sektoren eller ved udarbejdelse en adfærdskodeks. Ændringer i et direktivforslag om beskyttelse af personoplysninger og kommunikationshemmelighed i digitale telenet giver anledning til at advare mod, at nærhedsprincippet anvendes på en måde, der reelt fører til en udhuling af databeskyttelsen.

I dansk lovgivning findes en særlig regulering af betydning for elektroniske spor i lov om private registres særbestemmelser og i betalingskortloven. Der må vises særlig opmærksomhed for at sikre at disse bestemmelser kan opretholdes.

3. Elektroniske spor

I dette afsnit fremlægges en introduktion til elektroniske spor. Først søges nærmere afgrænset hvad elektroniske spor er og derefter beskrives nogle udviklingstendenser. I det følgende afsnit belyses trusler mod den personlige integritet. Endelig omtales reguleringen af elektroniske spor i lov om private registre.

3.1 Hvad er elektroniske spor?

Med elektroniske spor menes registreringer af personoplysninger i et edb-system. Med en udbredt anvendelse af edb i administrative og tekniske systemer i såvel den offentlige som i den private sektor vil der blive registreret personlige oplysninger om den enkelte i mange forskellige systemer. Sådanne registreringer findes i meget stort tal. Hvor stort vides ikke. Der findes omkring 1500 registre hos offentlige myndigheder, som har så følsomme oplysninger, at der er udarbejdet en registerforskrift. Desuden findes flere tusinde andre offentlige edb-registre. Antallet af registre hos private virksomheder mv. kendes ikke, men det anslås typisk, at det drejer sig om over ½ million. Endelig findes der registreringer i statistikregistre hos Danmarks Statistik og et ukendt antal forskningsregistre. Hvor mange registre den enkelte er registreret i vil naturligvis variere, men et forsigtigt gæt vil være mindst 150.

I nogen sammenhænge anvendes begrebet elektroniske spor som et udtryk for alle de elektroniske registreringer om den enkelte, der findes i forskellige systemer. Men her vil vi anvende begrebet om en del af disse registreringer[1].

Elektroniske spor henviser til edb-registreringer af typisk ikke-følsomme oplysninger i forbindelse med almindelige hverdagsaktiviteter. Et eksempel er registreringen af beløb og terminal når man benytter sit Dankort. De elektroniske spor opstår når man indfører edb til at administrere almindelige hverdagsaktiviteter, som f.eks. vareindkøb. De personoplysninger som registreres i edb-systemet er

ikke-følsomme oplysninger som identifikation, handlingen, beløb og lignende. I følge lov om private registre kan følsomme oplysninger (om rent private forhold) kun registreres når særlige betingelser er opfyldt, herunder samtykke.

Det er et kendetegn ved disse edb-systemer, at de anvendes af mange mennesker og at den enkelte benytter systemet mange gange. De elektroniske spor opstår netop fordi man vil opnå en forenkling af aktiviteter, som gentages i et betydeligt omfang. Systemerne vil derfor også typisk være opbygget så registreringen sker automatisk. Der er ingen personer involveret, som vurderer eller ser de personlige oplysninger som registreres i systemet. Dernæst er systemet opbygget med henblik på fortsat automatisk edb-behandling af de registrerede personoplysninger. I Dankort-systemet anvendes oplysningerne til postering af betalingerne.

Endelig er de elektroniske spor karakteriseret ved at registreringen er kendt i modsætning til en overvågning, hvor den forudsætningsvist ikke sker åben. Der er også her adgang til registerindsigt.

Med elektroniske spor henvises til registreringer af ikke-følsomme oplysninger i edb-systemer, der anvendes i forbindelse hverdagsaktiviteter, som foretages af mange mennesker og gentages ofte af den enkelte. Edb-systemer der danner disse elektroniske spor er karakteriseret ved at

- registreringen sker automatisk,
- der sker ikke en udvælgelse eller behandling af data i forbindelse med registreringen,
- de registrerede oplysninger anvendes til edb-behandling i umiddelbar forlængelse af aktiviteten og
- indsamlingen af data er kendt af den enkelte.

3.2 Udviklingstendenser

I takt med at edb tages i anvendelse på stadig flere område vil der opstå edb-systemer som danner elektroniske spor. Ofte vil et element i disse systemer være betalingsformidling.

De første mere udbredte elektroniske spor fremkom med udbredelse af elektroniske betalingskort, herunder først og fremmest pengeinstitutternes Dankort. Digitaliseringen af telefonnettet har betydet, at der nu dannes elektroniske spor, som viser hvilke telefonnumre der har talt sammen. Det forventes at vi står overfor en udvikling, hvor elektronisk kommunikation vil komme til at spille en stadig større rolle i hverdagen. Home-banking udbydes af de fleste banker. Tilbud om home-shopping er på vej. Det forventes at stadig flere vil benytte mange forskellige informations-serviceydelser. Når forbrugerne benytter tilbud, som er digitaliseret (edb-systemer, anvender informations-teknologi) opstår der muligheder for elektroniske spor.

Det er næppe muligt af afdække alle elektroniske spor og det er givet helt umuligt at forudsige de elektroniske spor der vil opstå i fremtiden. Men i takt med fremkomsten af informationssamfundet vil den enkelte i stigende grad kommunikere elektronisk, og der vil opstå stadig flere elektroniske spor - *med mindre der tages særlige initiativer*.

I afsnit 4 belyses eksempler på elektroniske spor i forskellige sammenhænge:

- betalingssystemer

- telefonsamtaler
- bibliotekslån
- trafikinformatik
- informations-serviceydelser.

3.3 Trussel mod den personlige integritet

De enkelte elektroniske spor er oftest i sig selv uden risiko for den personlige integritet. Men samles de elektroniske spor om en enkelt person er der mulighed for at tegne en detaljeret personprofil. Det bliver selvfølgelig endnu mere kritisk, hvis en sådan samkøring også omfatter personoplysninger i registre, der indeholder følsomme oplysninger. En sådan samkøring vil utvivlsomt været et voldsomt indgreb i den personlige integritet. Fremgangsmåden vil kunne danne grundlag for en detaljeret overvågning og kontrol af samfundets borgere i almindelighed eller særlige "afvigere" som det findes passende af holde nærmere øje med i særdeleshed.

Efter de eksisterende databeskyttelses-principper i Europarådets konvention og den danske registerlovgivning kan man næppe forestille sig en sådan samling af personoplysninger. Private registre må ikke samkøres, mens et tilsvarende forbud ikke findes for offentlige registre.

Det kan føre til den næste overvejelse om eksistensen af mange elektroniske spor er ønskelig eller acceptabel. Hvis elektroniske spor bliver ganske udbredt vil de indeholde oplysninger om mange af de aktiviteter den enkelte foretager sig i privatlivet. Det kan opleves som et stort ubehag, at oplysningerne overhovedet findes et sted. Som det hedder med et mundheld: "Ingen har lyst til at bo i et glashus". Registreringen kan skabe en frygt og usikkerhed hos den enkelte som forringer tryghed og livskvalitet.

Set fra en samfundsmæssig vinkel kan man spørge om det er fornuftigt at der dannes meget store mængder elektroniske spor, som det er *teknisk muligt* at finde frem og samkøre. Det må også overvejes om et retlig værn mod misbrug i form af forskellige retsregler er tilstrækkelig sikkerhed. Sådanne regler kan jo ændres under skiftende politiske og samfundsmæssige forhold.

De elektroniske spor kan blive en trussel mod den personlige integritet ved forskellige ændrede anvendelser. De personlige oplysninger kan anvendes til andre formål end det de umiddelbart er registreret til. F.eks. har det været diskuteret om bankerne kan anvende oplysninger fra Dankort-transaktioner, som findes på kundernes kontooversigt, i forbindelse med kreditvurdering.

En anden "ny" anvendelse er markedsføring. Systemejeren kan anvende oplysningerne til kontakt til kunderne med ny tilbud. Oplysninger kan også videregives til andre virksomheder der ønsker at sende reklamer eller til virksomheder der gennemfører mikromarketing på baggrund af oplysninger fra mange kilder.

Den personlige integritet kan krænkes ved at personoplysninger kommer til uvedkommendes kendskab. Der kan være tale om personer hos systemejeren, som skaffer sig adgang til oplysninger og bruger dem på en uautoriseret måde. Eller der kan være tale om folk uden for systemejerens virksomhed, som ved

indbrud, hacking eller lignende skaffer sig personoplysninger. Videre kan personoplysninger komme uvedkommende i hænde ved en fejl, f.eks. ved at uddata-materiale findes på en losseplads efter de er kasseret.

Personoplysningerne kan tænkes anvendt til kriminelle formål f.eks. til at skaffe viden om hvor det kan betale sig at lave indbrud eller som grundlag for pengeafpresning.

Endelig kunne man tænke sig at efterretningstjenester får adgang til personoplysninger i elektroniske spor til overvågningsvirksomhed.

Igennem lovgivning på forskellige områder er disse trusler søgt imødegået. Generelt reguleres elektroniske spor af loven om private registre, som behandles i næste afsnit. Elektroniske spor i forbindelse med betalingskort og betalingssystemer har påkaldt sig særlig interesse og er reguleret i en særlig lov, betalingskortloven (se afsnit 4.1). Spørgsmålet om anvendelse af almindelige oplysninger (elektroniske spor og andre registreringer) til markedsføringsformål er reguleret ved særregler i lov om private registre og for offentlige registre f.eks. ved særregler i lov om det centrale erhvervsregister og tinglysningsloven.

3.4 Lov om private registre

Elektroniske spor hos private virksomheder vil være omfattet af lov om private registre[2].

En virksomhed må registrere personlige oplysninger når det er et naturlig led i virksomhedens naturlige drift. Virksomhedens interne anvendelse af oplysningerne er ikke reguleret.

Oplysninger kan videregives når det er et naturligt led i virksomhedens naturlige drift. Videregivelse kan også ske efter samtykke fra den registrerede. Som hovedregel må der ikke videregives oplysninger om forbrugere til brug for markedsføring. Videregivelse kan dog ske, når den registrerede har givet udtrykkelig samtykke på baggrund af en skriftlig meddelelse fra virksomheden. Samkøring af edb-registre fra forskellige virksomheder er ikke tilladt.

De oplysninger der registreres skal være korrekte. Urigtige og vildledende oplysninger skal rettes eller slettes. Oplysninger, der er uaktuelle på grund af alder eller af andre grunde, skal slettes.

Alle, som mener de er registreret i et edb-register, har ret til ved henvendelse til virksomheden at få oplyst, hvad der er registreret.

4. Eksempler på elektroniske spor

I dette afsnit belyses eksempler på elektroniske spor i forskellige sammenhænge. Der er ikke tale om et forsøg på en samlet beskrivelse af alle elektroniske spor i samfundet. Men eksemplerne giver forhåbentlig et overblik, som kan danne grundlag for overvejelser om politiske initiativer og yderligere vurderingsinsats.

4.1 Betalingssystemer: Hvad har du lavet?

Mange hverdagsaktiviteter er knyttet sammen med betalinger. Når man står i forretningen eller andre steder kan man selvfølgelig vælge at betale med sedler og mønter fra pungen. Men elektroniske betalinger har som bekendt vundet frem. Dankort og andre betalingskort anvendes til betalinger, og småpengekortet, DANMØNT kan benyttes stadig flere steder til betaling af mindre beløb. Men hverdagsaktiviteterne kommer i stigende grad til at omfatte, at vi kommunikerer elektronisk. Bankforretninger kan klares med telefonen eller fra pc'en. Det forventes, at vi vil købe varer, bestille billetter og modtage tjenesteydelser via elektronisk kommunikation. Der skal betales for den vare eller tjenesteydelse som modtages. Hvor og hvordan den enkelte har betalt for forbrug kan få form af elektroniske spor. I dette afsnit behandles først tre former for elektronisk betaling og dernæst behandles betalingskortlovens regulering af data i betalingssystemer.

4.1.1 Elektronisk betaling

I det følgende beskrives tre principielt forskellige måder at udforme den elektronisk betalinger på:

- betalingskort
- forudbetalte kort
- anonyme betalinger.

Betalingskort

Med betalingskort tænkes her på Dankort, Veko-kort, Finax-kort og tilsvarende betalingskortsystemer. Selvom systemerne på mange måder er udformet meget forskelligt har de det fælles træk, at betalingerne gennemføres via et særligt betalingssystem, som formidler betalings-beløbet overført fra forbrugerens konto til sælgerens. Ved betalingen registreres oplysninger, som er knyttet til den enkelte og vil kunne indeholde detaljerede oplysninger om forbruget. Men, som omtalt nedenfor, er det i betalingskortloven fastsat, at selve forbruget, f.eks. hvilke varer der er købt, ikke må registreres. Ved denne form for elektronisk betaling dannes således elektroniske spor.

Det elektroniske spor registreres først hos PBS. Ved daglige opdateringskørsler formidles betalingerne til bankerne, og det elektroniske spor ender med en registrering i forbrugerens bank. Bankerne registrerer dato, terminal hvor beløbet er hævet og beløbet.

Bankerne oplyser, at deres rutiner foreskriver at terminal (hvor beløbet er hævet) kun oplyses som et nummer overfor bankens personale. Personalet vil kun i sager med tvivl om rigtigheden af konteringen

afkode det pågældende terminalnummer. På kontoudtog udskrives, som en service for kunden, i tekst hvor pengene er hævet.

Forudbetalte kort

En anden måde at organisere elektroniske betalinger på er med forudbetalte kort. Et sådant system introduceres i Danmark af firmaet DANMØNT. I systemet anvendes computerkort, dvs. plastkort med en indbygget computer eller hukommelse. Systemet fungerer ved at forbrugeren køber et småpengekort med beløb på f.eks. 50 eller 100 kr. Når kortet anvendes tælles beløbet i kortet ned. På terminalen informeres brugeren om det aktuelle betalings-beløb og restbeløbet på kortet. Danmønt kortet er tænkt til betalinger af småbeløb (indtil ca. 50 kr.) i kiosker, vaskerier, busser, telefoner, automater til billet eller fødevarer og lignende.

Ved anvendelse af DANMØNT dannes der ikke elektroniske spor. Der er ikke knyttet en personlig identifikation eller pin-kode til det enkelte kort.

DANMØNT kan anvendes i 44 byer og der blev i 1 kvartal af 1995 gennemført over 400.000 transaktioner [3].

Firmaet Danmønt er systemoperatør og udsteder kortene og formidler betalingerne. Systemoperatøren er ansvarlig for sikkerhed og troværdighed for hele systemet.

Et EU støttet projekt, CAFE (Conditional Access for Europe) har bl.a. en tilsvarende småpenge-funktion. Dette system baseret sig på en teknik med blinde digitale signaturer, som beskrives i næste afsnit [4].

Anonyme betalinger

Der er udviklet et alternativt elektronisk betalingssystem ved brug af informationsservice-ydelser[5] af bl.a. firmaet DigiCash i Holland.

Ideen i betalingssystemet er, at man får elektroniske penge eller værdi-kuponer fra banken, som ved udleveringen fratrækker beløbet på kontohaverens konto. Værdikuponerne er stemplet af banken med beløb og bankens digitale underskrift. På den måde garanterer banken, at den senere vil indløse den elektroniske værdikupon med det pålydende beløb. Når man skal betale for en informations-serviceydelse fremsender man en eller flere elektroniske værdikuponer til udbyderen, som derefter kan sende dem til sin bank, som overfører beløbet til kontoen.

Betalingerne er anonyme, da de elektroniske værdikuponer ikke bærer spor af den (eller de) personer, der har anvendt dem. Når informationservice-udbyderen og derefter banken har modtaget værdikuponen er det ikke muligt at se hvilke betalinger der hører til hvilke konti/personer f.eks. ved søge gennem værdikuponerne eller ved læse de enkelte kontobevægelser. På kontooversigten vil kun fremgå, at er der hævet (elektronisk) et antal elektroniske værdikuponer.

Betalingerne er anonyme, fordi bankens underskrift på den elektroniske værdikupon er en såkaldt blind underskrift. Værdikuponerne fremsendes af forbrugeren til banken i en standardiseret form bl.a. indeholdende et skjult nummer. Dette nummer, kan banken ikke læse og derfor heller ikke registrere. Banken påfører værdikuponen det beløb forbrugeren har bestilt og sin digitale underskrift. Underskriften er blind i den forstand, at banken ikke kender nummeret på den værdikupon, som den underskriver. Den

elektroniske værdikupon sendes herefter retur til forbrugeren og beløbet fratrækkes kontoen. Der er herefter ingen forbindelse mellem forbrugerens konto og værdikuponen. Værdikuponen udpakkes af forbrugerens edb-program og består nu af et nummer, beløb og bankens underskrift. Det er denne udgave af den elektroniske værdikupon, som ender hos banken og udløser en betaling.

I en virkelig implementering er systemet mere kompliceret end det er beskrevet her. Det skal nævnes, at der er procedurer, som sikrer at en værdikupon er ægte og kun benyttes én gang.

Et betalingssystem med anonyme elektroniske penge eller værdikuponer anvender public key kryptering til dannelse af digitale underskrifter og den særlige form for blinde underskrifter.

4.1.2 Betalingskortloven

Betalingskortloven [6] gælder for "betalingssystemer med betalingskort, samt betalingssystemer, der kan sidestilles hermed, som udbydes eller kan benyttes her i landet" (§1 stk. 1)

Betalingssystemer

Loven omfatter således alle former for elektroniske betalingssystemer og ikke kun systemer hvori indgår et plastkort. Loven burde egentlig ikke hedde betalings*kort*loven, men snarere lov om elektroniske betalingssystemer. Den seneste ændring af loven i 1994 tog udgangspunkt i udbredelse af homebanking og en forventning om udbredelse af elektronisk betaling på andre områder, f.eks. home-shopping.

Der findes ikke en egentlig definition af betalingssystem i loven og der findes endnu ikke en praksis, som nærmere fastlægger hvilke systemer, der vil blive opfattet som betalingssystemer. I stk. 2 afgrænses til "betalingssystemer uden betalingskort, men med kode eller andet lignende legitimationsmiddel..". Sådanne elektroniske betalingssystemer er "typisk konstrueret således, at det er muligt uden kontakt med en fysisk person ad elektronisk vej at anvende systemerne i betalingsøjemed, således at brugeren kan foretage betalingsoverførsler, hæve penge, købe eller sælge valuta eller værdipapirer, erhverve varer eller tjenesteydelser eller gennemføre lignende transaktioner" [7] Begrebet "betalingsøjemed" opfattes bredt, "dvs. at såvel direkte overførsel af betaling fra/til bankkonti som en registrering og opsamling i systemet af fordringer på brugeren til efterfølgende betaling via andre betalingskanaler - parallelt til eksempelvis visse konto- og kreditkort - forstås som en betaling i lovens forstand" (Bet. 1255 s. 38f.).

Betalingskortloven regulerer selvfølgelig de kendte betalingssystemer med anvendelse af plastkort, f.eks. Dankort-systemet og forskellige kreditkort, herunder vaskerikort i en boligforening. Det er videre opfattelsen, at loven omfatter småpengekort, som DANMØNT. Det er videre vurderingen, at TeleDanmarks system til opkrævning af betaling for de såkaldte 900-tjenester er et betalingssystem i lovens forstand. Det er ligeledes opfattelsen, at Diatels system til opkrævning af betaling af forbrugsafgifter for forskellige serviceydelser er et betalingssystem i lovens forstand.

Som en slags modstykke til det meget brede betalingssystem-begreb indeholder loven mulighed for at give dispensation helt eller delvist fra lovens bestemmelser. "Det vil således være hensigtsmæssigt i en forsøgsperiode, at kunne dispensere helt eller delvist fra loven fsv. angår elektroniske systemer, hvor der sker en registrering og opsamling af fordringer på brugeren, men hvor betalingselementet alene er afregning for brug af det elektroniske systems primære funktioner. Som eksempler herpå kan nævnes telekommunikationstjenester fx. kontoopkaldsystemer, edb-biblioteker og andre lignende

informationssystemer, hvor brugeren ved hjælp af et modem, har adgang til informationer, diverse edb-programmel, eller databaser med søgefunktioner som fx. Retsinformation, UNI-C m.fl. .." (Bet. 1255 s.65)

Registrering, anvendelse og videregivelse af oplysninger

Behandlingen af personoplysninger i betalingssystemer er omfattet af lov om private registre og bestemmelserne i betalingskortloven supplerer disse bestemmelser. I følge lov om private registre må erhvervsvirksomheder registrere oplysninger som er nødvendige for virksomheder af pågældende slags. Loven regulerer ikke den interne anvendelse af disse oplysninger; oplysningerne skal slettes når de er uaktuelle.

Betalingskortloven giver et nærmere indhold: Der må kun registreres oplysninger som er nødvendige for gennemførelse af betalingstransaktioner. Det må derfor f.eks. ikke registreres hvilke varer der er købt. Oplysningerne må kun anvendes til betalingstransaktionen, hvorved den interne anvendelse er reguleret. Tilsvarende må oplysningerne kun videregives for at gennemføre betalingstransaktionen. Oplysninger må opbevares i 5 år, hvorefter de skal tilintetgøres.

Revision

Man er opmærksom på, at betalingssystemer er et nyt område, som vil udvikle sig på en måde der næppe kan forudses. Der er derfor indsat en revisions-bestemmelse i loven. Forslag om revision af loven skal fremsættes i folketingsåret 1997-98.

4.2 Telefonsamtaler: Hvem snakker du med?

Digitaliseringen af telefoncentralerne blev startet i begyndelsen af 1980'erne i Danmark. Idag er ca. 50% af abonnenterne tilsluttet en digitalcentral. Det forventes at digitaliseringen er gennemført inden år 2010.

Med de digitale centrale blev indført en funktion med overførsel af A-nr. Dvs. den kaldende abonnents nummer fremføres gennem telenettet. Fra begyndelsen af 1990'erne er denne funktion også indbygget i de analoge telefoncentraler, således at A-nr (kaldende abonnents telefonnummer) kan fremføres og anvendes for alle abonnenter [8].

Denne ny facilitet i telefonnettet anvendes internt af TeleDanmark til dirigering af samtalen, taksering og sporing. Funktionen er grundlag for en række tjenester, som TeleDanmark udbyder, bla. "closed user group", hvor kun forudbestemte abonnenter kan ringe op til et bestemt nummer. Tjenesten kan anvendes som en sikkerhedsforanstaltning f.eks. ved opkobling til edb-systemer. Telefonnummeret kan også fremføres til den opkaldte abonnent og f.eks. vises på et display [9].

A-nr. overførslen er først og fremmest anvendt til tjenesten specificeret regning. Tidligere registrerede man abonnentens forbrug som tællerskridt. Med indførelse af A-nr. registrerer man hvilket telefonnummer der er ført en samtale med, og så selvfølgelig tidsrummet. På grundlag af denne registrering er det muligt at udskrive en specificeret regning over hvilke samtaler regningsbeløbet

dækker.

Indførelse af funktionen A-nr. har medført, at der dannes et elektronisk spor efter enhver telefonsamtale. I TeleDanmarks edb-system dannes et register over hvilke telefonnumre en given telefon har ført samtaler. Selvom det er telefonnummeret og ikke direkte personen, som registreres, er der på grund af den indirekte sammenhæng mellem et telefonnummer og pågældende abonnent tale om registrering af personoplysninger. Registreringerne opbevares 1 år hos telefonselskabet.

Denne registrering af telefonsamtaler har ikke givet anledning til større debat [10].

Registrering af telefonnumre blev reguleret i lov private registre §7f ved ændring af loven i 1987. Baggrund for reguleringen var spørgsmålet om arbejdsgiverens mulighed for at registrere medarbejdernes samtaler. Det er forbudt virksomheder at foretage automatisk registrering af telefonnumre, som der ringes til. Telefonselskaber må dog registrere telefonnumre med henblik på betaling og teknisk kontrol. Telefonselskaberne kan tilbyde en specificeret regning, som angiver opkaldt telefonnummer, klokkeslet, samtalens varighed og pris. Denne ordning må ikke benyttes af virksomheder, da de ikke selv må foretage denne registrering. Den specificerede regning kan tilbydes private, da deres registrering ikke er omfattet af loven. Videregivelse iøvrigt kan ikke anses for tilladt uden samtykke.

I forslag til EU direktiv om beskyttelse af personoplysninger i offentlige telenet hed det i det oprindelige forslag: [11] "Teselskaberne må kun foretage indsamling, opbevaring og behandling af personoplysninger, hvor dette sker med henblik på telekommunikation, navnlig med henblik på opsættelse af kald til transmission af tale, data, og billeder, udskrift af regninger, eller andre legitime formål, der er nødvendige af hensyn til driften, herunder fejlretning, sikring af teleselskabets udstyr mod forkert brug samt registrering af indkommende opkald" (artikel 4) og i stk. 2: "Teleselskabet må ikke bruge disse oplysninger til at udarbejde elektroniske profiler over abonnenterne eller klassificere individuelle abonnenter i kategorier."

I Kommissionens ændrede forslag fra 1994 [12] er bl.a. denne generelle bestemmelse om behandling af personlige oplysninger "slettet for at tilgodese nærhedsprincippet". Direktivet indeholder fortsat bestemmelser on debiteringsdata, trafikdata og om specificerede samtaleopgørelser.

Om debiteringsdata fastsættes i artikel 5:

> "1. Med henblik på debitering er det tilladt at behandle debiteringsdata, der indeholder abonnentterminalens telefonnummer eller identifikationsnummer, abonnentens adresse og terminaltype, det samlede antal debiteringsenheder for afregningsperioden, det kaldte apparats nummer, samtalernes type og varighed og/eller mængden af transmitterede data, samt anden information, der er nødvendig i forbindelse med debiteringen, herunder oplysninger om forudbetaling, ratevis afregning, lukning og rykkerskrivelser. Kun personer med ansvar for debiteringen må have adgang til sådanne lagrede data.
>
> 2. En sådan generel opbevaring af debiteringsdata er tilladt indtil udløbet af den lovhjemlede forældelsesfrist for sådanne gældsforpligtigelser."

Direktivet har siden 1994 ventet på afklaring af det generelle direktiv om beskyttelse af personoplysninger.

4.3 Biblioteket: Hvad læser du?

Når man låner bøger og andet materiale på folkebibliotekerne må de nødvendigvis registrere hvilke bøger man har lånt. Denne udlånskontrol er gennem de senere år omlagt til edb og dermed dannes der elektroniske spor efter borgernes biblioteks-lån.

I et produktblad om Kommunedata's system "UNI MASTER" beskrives systemet således:

> "Udlånsrutinerne omfatter: udlån, aflevering, fornyelse og reservering; samt diverse udskrifter f.eks.: hjemkaldelser, reservationsmeddelelser, liste over materialer på reservationshylderne m.m.

Til en hver tid er det muligt at foretage en lånerstatus på en enkelt låner vedrørende hjemlån, reservering eller evt. mellemværende"

En offentlig myndighed må kun registrere oplysninger som klart er af betydning for varetagelse af myndighedens opgaver [13]. Ved en ændring af lov om offentlige myndigheders registre i 1991 blev registre, som ikke indeholde fortrolige oplysninger, fritaget for kravet om udarbejdelse af registerforskrift (jfr. §§8a-e). Disse registre må dog indeholde identifikationsoplysninger, typisk personnummer, og oplysninger om betalingsforhold.

I Justitsministeriets bekendtgørelse om visse typer af offentlige edb-registre [14] fastsættes om bibliotekssystemer:

> "Registre, der anvendes ved administration af udlån m.v. på biblioteker, og som ikke indeholder andre end følgende oplysninger om låneren, jfr dog §2 [identifikationsoplysninger og oplysninger om betalingsforhold]:
> 1) Oplysninger om låneren og udlånet m.v., såfremt der er forbindelse mellem de enkelte udlån m.v. og låneren slettes snarest og senest 4 uger efter udlånets ophør. Ved udlån efter en særlig serviceordning kan registreringen med lånerens skriftlige samtykke opretholdes i op til 3 år./../"

Registreringen af bibliotekslån er således nærmere reguleret og det er fastsat at oplysningerne skal slettes.

4.4 Trafikinformatik: Hvor har du været?

I Vejdatalaboratoriets blad vdl-nyt introduceres trafikinformatik med, at det handler om at håndtere data om og for trafik. "Det er der tilsyneladende ikke noget nyt i. Vi har i mange år beskæftiget os med trafikdata i form af blandt andet tællinger, analyser og modeller. Det er derfor vigtigt for os at markere, at det nye begreb er bredere end de traditionelle trafikregistreringer. Det omfatter for eksempel også alle informationer, der har betydning for, hvordan trafikken afvikles. Det kan være oplysninger om vejret, føret, trafikuheld eller vejarbejder. Dertil kommer oplysninger om selve vejnettet og det tilhørende rutemuligheder" [15]

Med trafikinformatik skabes mulighed for elektronisk kommunikation mellem den enkelte trafikant og forskellige edb-systemer. Interessen har været koncentreret om vejtrafikken. Bilerne får indbygget computere og der bliver mulighed for kommunikation mellem bilen og sendere ved vejen eller via satellitter. Trafikinformatik er et relativt nyt område, som vi først er ved at se de første anvendelser af. En tidskritisk faktor er netop udstyret i bilerne, som det tager en længere årrække at få udbredt.

Men der lægges stor vægt på at udbrede trafikinformatik. I Bangemann rapporten til EU-Ministerrådet anbefales 10 applikationer, der skal bane vejen for informationssamfundet. Bl.a. "Vejstyring. Edb-Styret trafik giver bedre livskvalitet", hvor det anbefales, at "der udvikles telematiksystemer i europæisk skala til avanceret vejtrafikstyring og andre transporttjenester (førerinformation, rutevejledning, flådestyring, vejafgifter, mv.)" [16] Tilsvarende hedder det i regeringens IT-handlingsplan i et afsnit om "Bedre trafik med IT", at "Trafikministeriet iværksætter en række forsøgs- og udviklingsprojekter om trafikinformatik.." [17]

Indførelse af informations- og kommunikationsteknologi i trafikken åbner mulighed for en registrering af personlige oplysninger i en række sammenhænge: registre med betalingsforhold i.f.m. vej- og parkeringsafgifter, trafikregistrering, trafikinformation og hastighedsovervågning. Udvikling af trafikinformatiksystemer sætter spørgsmålet om registrering af vores fysiske færden på dagsordenen.

Hvordan vil vi opfatte registrering af vores tilstedeværelse? I registerlovenes beskrivelse af følsomme, rent private oplysninger er ikke medtaget sted; og trafikinformatik-systemers registrering af personoplysninger vil derfor være omfattet af de almindelige betingelser for registrering.

I hvilken udstrækning de trafikinformatik-systemer, som kommer i drift, vil indebære elektroniske spor må idag siges at være et åbent spørgsmål.

I slutdokumentet fra TeknologiNævnets konference "På vej mod intelligent trafik" hedder det: "Fordi en række trafikinformatiksystemer bygger på indsamling og behandling af personoplysninger, vil der komme en række nye registreringer. Det kan være registre med betalingsforhold i forbindelse med vejafgifter, trafikregistrering og identifikation af køretøjer og trafikanter.

Til registrering i forbindelse med for eksempel hastighedsovervågning er kun identifikation af køretøj nødvendig.

De nuværende registerlove sikrer, at kun relevante personer og instanser har adgang til registrerede personoplysninger.

De nye registre har måske begrænset betydning, men der ligger en risiko i, at de bringes sammen. Aktuelt er dette ikke lovligt, men der er et bestandigt pres for at udnytte mulighederne i de registrerede data.

Når der oprettes databaser, er det vigtigt, at der kun indsamles data, som er nødvendige i forbindelse med trafikinformatiksystemets funktion.

Vi kræver, at der skal være frivillighed i forhold til systemer, der registrerer personer. En så høj grad af anonymisering som mulig bør tilstræbes"[18] I de følgende afsnit behandles kort nogle eksempler på trafikinformatik-systemer, som indebærer dannelse af elektroniske spor.

Bompenge

Betaling for kørsel på bestemte veje, f,eks. motorveje eller ved indfaldsveje til byområder er indført i flere lande og overvejes også i Danmark. Det er besluttet at der skal betales afgifter ved kørsel på de ny broer over Storebælt og Øresund.

Det er muligt at gennemføre betalingen mens bilen passerer opkrævningsstedet i normal hastighed. I bilen findes en terminal, som etablerer en kommunikation med antenner ved siden af eller over vejen ved betalingsstedet.

Vejafgiftssystemet kan fra en registreringssynsvinkel opbygges efter forskellige principper: en forudbetaling, en kontoordning eller et betalingskort.

Ved en *forudbetaling* kan trafikanten købe et månedskort, klippekort eller lignende typisk i form af et computer-plastkort. Når betalingsstedet passeres kontrolleres månedskortet eller klippekortet tælles ned. Forudbetalingen vil normalt betyde, at der ikke blive foretaget en personregistrering.

Med en *kontoordning* vil betalingssystemet registrere bilisten og samle betalingerne på en konto, som fremsendes hver måned.

Endelig kan betalingsstedet fungere som et *betalingssystem*, dvs. det får oplysninger fra bilistens betalingskort og betalingen gennemføres på samme måde som en betaling i en forretning.

Vejskat

Når bilerne kan kommunikere vil det være muligt mere generelt at omlægge beskatningen fra skat på bilen til skat på brugen af den. Det kunne f.eks. motiveres med miljøhensyn, og man kunne derfor ønske at graduere skatten efter hvor og hvornår bilen blev anvendt.[19]

Systemet kunne opbygges med en central registrering af hvor bilen blev anvendt, hvilke veje er der kørt af og på hvilke tidspunkter. På den måde kunne man ud fra opstillede regler foretage en beskatning på baggrund af bilens anvendelse og miljøbelastning.

Trafikinformation

Et andet område i trafikinformatikken er oplysning til trafikanterne om valg af rute, og oplysninger om forhold af interesse på ruten f.eks. vejr, bilkøer, trafikuheld o.l.

Sådanne systemer kunne bygges ved at bilisten på en strækning "melder" sig og giver forskellige oplysninger, herunder hvor vedkommende er på vej hen. Informationssystemet vil herefter kunne sende trafik-oplysninger til bilisten. Samtidig vil systemet kunne anvende bilistens oplysninger til forudse trafikproblemer.

4.5 Informationsservice-ydelser: Hvad har du efterspurgt?

I de kommende år vil der utvivlsomt ske en betydelige udbredelse af informationsservice-ydelser, som benyttes fra hjemmets pc. Pc'en kan, når den er udstyret med et modem, kommunikere med udbydernes edb-systemer via telenettet.

Man kan forvente et bredt spektrum af serviceydelser: varekøb, bankforretninger, underholdning, tv/video on demand, elektronisk post, nyheder, informationer, selvbetjening hos offentlige myndigheder m.m.

Der vil komme "elektroniske markedspladser", som udbyder en samlet indgang til en række serviceydelser. I starten af 1995 åbnede Diatel som "er et elektronisk indkøbs- og informationscenter, hvor du kan købe ind - døgnet rundt". Det er kendt at Microsoft forbereder et internationalt tilbud om en "elektronisk markedsplads". I USA har IBM og Sears opbygget Prodigy med en lang række informationsservice-ydelser. En amerikansk undersøgelse forudser, at i 2009 vil halvdelen af al handel i USA forgå gennem informationsservice-systemer som Prodigy [20].

Her er fokuseret på anvendelsen af en pc, som apparat i hjemmet. Men der udbydes allerede en række serviceydelser med anvendelse af telefonen. Da trykknaptelefonen er meget udbredte i Danmark er der et godt grundlag for denne form i Danmark.

Informationsservice-ydelser baserer sig på, at to computere sender data over telenettet til hinanden. For at disse data bliver sendt til den rigtige computer anvendes forskellige former for adresser. Allerede her ligger der i teknikken en mulighed for at registrere oplysninger om brugen af serviceydelsen med modtagerens identifikation. Dernæst vil man af sikkerhedsgrunde typisk kræve, at den der ønsker at benytte en informationsservice-ydelse identificerer sig før pågældende får adgang til systemet. Denne identifikation kan ligeledes danne grundlag for en registrering. Ved anvendelse af informationsservice-ydelser vil den enkelte videre typisk være oprettet som bruger hos udbyderen og dermed kan forbruget registreres. Ved anvendelser, hvor der betales for tidsforbrug vil der selvfølgelig ske en registrering heraf. Informationsservice-ydelsens computer har under brugen af ydelsen adgang til alle oplysninger om denne brug og detaljeringen af en registrering er et systemvalg, som udbyderne foretager - inden for rammerne af lovgivningen.

Diatel oplyser "om de informationer, som Diatel opbevarer om kunderne:

> Diatel registrerer ved tilmelding en række basisoplysninger til brug for vort bogholderi. Det drejer sig om navn, adresse, telefonnummer og - hvis der er tale om overførsel via BetalingsService - kundens kontonummer.
>
> I forbindelse med kundens brug af Diatel-services registreres det nødvendige grundlag for evt. senere fakturering, d.v.s. tidspunkt for servicekald, tidspunkt for afslutning af service, evt. forekomster af 'klikafgifter' (tidsuafhængig forbrugsafgift).
>
> Disse oplysninger opbevares under meget høj sikkerhed. Diatel's centrale computer er placeret i Kommunedata's maskinstue. Oplysningerne opbevares i overensstemmelse med Bogføringslovens krav til dette - d.v.s. p.t. 5 år."

Mulighederne i registreringen kan illustreres med det omtalte system, Prodigy i USA.

> "Prodigy abonnenterne bliver registreret på en sådan måde, at det er muligt at lave reklamer på systemet, som henvender sig til særlige kundekategorier. Når man tegner abonnement på Prodigy, skal man give enkelte personoplysninger, og derudover registrerer systemet, hvilke interesseområder brugeren har. Det sker ved at lagre oplysninger om de tjenester, brugeren benytter og dermed interesseområder, brugeren har.
>
> Hvis man ofte søger oplysninger om rejser, er det oplagt, at abonnenten skal se nogle rejsereklamer. Hvis man flere gange leder efter information om sundhed, skal abonnenten have reklamer for naturmedicin. Der kan altså tegnes en profil af den enkelte bruger, og de reklamer, som iøvrigt optræder som en appetitvækker nederst på skærmbilledet, kan derfor målrettes i forhold til forskellige typer af brugere.
>
> I USA er den form for direct mailing almindelig, men i Europa er der nærmest tale om et skræmmebillede."[21]

Hvilke registreringer og anvendelser vi vil se her hjemme kan der næppe siges noget helt præcist om.

Med revisionen af betalingskortloven i 1994 blev en informationsservice-ydelser, som er et betalingssystem, omfattet af loven (jfr. afsnit 4.1.2).

Registreringer, der ikke er omfattet af betalingskortloven, vil være omfattet af lov om private registre (jfr. afsnit 3.4). Betingelsen for registreringen er, at den er en naturlig led i virksomhedens normale drift. Der stilles ikke særlig skrappe krav for at opfylde dette formål. Når registreringen er foretaget regulerer loven ikke virksomhedens interne anvendelse, og man kan derfor tænke sig, at registreringen benyttes til markedsføringsformål og elektroniske tilbud. Såfremt det blive en normal praksis, at informationsservice-udbydere registrerer kundernes brug af systemet, vil der, med en udbredt brug af elektroniske informationsservice-ydelser til mange sider af hverdagslivet, komme en betydelig udbredelse af elektroniske spor.

5. Handlemuligheder

I afsnit 3.1 behandledes risici for indgreb i den personlige integritet ved elektroniske spor. Det blev nævnt, at der i en række love er foretaget en regulering af forskellige elektroniske spor. Det kan konstateres, at der er en generel politisk accepteret målsætning om, at udbredte elektroniske spor udgør en risiko, som bør imødegås.

Denne databeskyttelses-politik kan gennemføres på to måder. For det første kan man søge helt at undgå at der dannes elektroniske spor, og for det andet kan man tilvejebringe en regulering af de elektroniske spor som dannes.

5.1 Undgå elektroniske spor

En oplagt og effektiv måde at imødegå risici for den personlige integritet ved elektroniske spor er helt at undgå at de dannes. Her tænkes ikke på, at man undlader at anvende edb, men tanken er, at de edb-baserede systemer udformes så der ikke dannes elektroniske spor. De systemer vi behandler her er typisk udarbejdet ud fra en interesse for at få løst en given opgave effektivt til færrest mulige omkostninger, og ikke ud fra en interesse i at have adgang til de personlige oplysninger der registreres. Med udgangspunkt i denne "systeminteresse" bør der være grundlag for at opbygge systemer som ikke registrerer personlige oplysninger.

I afsnit 4.1 blev omtalt forudbetalte kort og anonyme betalinger som eksempler på betalingssystemer, der ikke medfører elektroniske spor. I afsnittet om trafik-informatik (4.4) blev omtalt muligheden for at tilrettelægge f.eks. vejafgifts-systemer på en sådan måde, at der ikke blev dannet elektroniske spor.

Systemet med anonyme betalinger anvender en systemudformning, der omtales som "blinde signaturer"[22]. Denne teknik kan også anvendes i andre sammenhænge til at opbygge edb-systemer, hvor de registreringer der foretages ikke kan henføres til bestemte personer. Blinde signaturer bygger på public key kryptering, som er en teknik der generelt vinder stor udbredelse i disse år, og, som det derfor må vurderes, vil være relativt enkelt at indføre. Videre vil det for nogle systemer forudsætte, at brugerne har et computer-kort. Sådanne kort - og tilhørende kortlæsere - må forventes at få betydelig udbredelse i de kommende år, jfr. overvejelserne om et dansk borgerkort. De tekniske forudsætninger er således tilstede, for at sådanne edb-systemer på nye områder kan udformes så der ikke dannes elektroniske spor.

Der er her peget på to løsninger for systemer uden elektroniske spor, men der kan ganske givet også udformes andre løsninger.

Systemerne udformes inden for gældende lovgivning af systemejerne. Der findes (naturligvis) ikke et forbud mod elektroniske spor, tværtimod findes der lovgivning som regulerer registrering af personlige oplysninger. Private virksomheder og offentlige myndigheder beslutter på dette grundlag og ud fra en samlet vurdering, hvordan systemet skal udformes. I hvilken udstrækning databeskyttelseshensyn i almindelighed, og målsætninger om at undgå elektroniske spor i særdeleshed, indgår er det næppe muligt at sige noget generelt om, men det kan frygtes, at det ikke vil spille en særlig stor rolle. Der mangler derfor fremgangsmåder, som kan sikre, at der tages stilling til om systemet behøver at registrere

personoplysninger, og fremme systemdesign som ikke indebærer elektroniske spor.

En mulighed kunne være, at systemer af den type, som er beskrevet i afsnit 3.1, forudsætter en udtalelse fra Registertilsynet, som bl.a. bør indeholde overvejelser om hvorvidt registrering af personoplysninger helt bør undgås.

5.2 Regulering af sporene

Elektroniske spor er som udgangspunkt reguleret af registerlovene.

Offentlige registre

Offentlige registre er oprettet i henhold til lovgivning. I forbindelse med denne lovgivning er der mulighed for at fastsætte nærmere regler for de elektroniske spor, hvilket tilsyneladende sker i stigende omfang.

Edb-registeret kan videre kun oprettes efter en procedure som inddrager Registertilsynet, der har lejlighed til at udtale sig om udkastet til register-forskrift. Den endelige register-forskrift fastsættes efter beslutning af en politisk instans, som kan gøres ansvarlig i en åben demokratisk debat.

Elektroniske spor vil ofte optræde som ikke-følsomme registre (jfr. bibliotekslån i afsnit 4.3), og må antages at være omfattet af nærmere regler i bekendtgørelse eller cirkulære.

Private registre

Private virksomheders registreringer er reguleret af lov om private registre, der fastsætter en retlig standard for registrering af personlige oplysninger. Denne retlige standard vil oftest være utilstrækkelig til at regulere mere omfattende elektroniske spor. Desuden findes der i loven ingen regulering af virksomhedens interne anvendelse af lovligt registrerede oplysninger.

Det kan derfor også konstateres, at der i loven er optaget særregler for en række virksomheders registreringer. Videre er der for elektroniske spor i betalingssystemer foretaget en særlig regulering i betalingskortloven.

På det grundlag må det vurderes, at der ved fremkomst af mere omfattende systemer med elektroniske spor vil være behov for en specifik regulering. [23]

Med udgangspunkt i betalingskortloven kan en sådan regulering omfatte

- en nærmere afgrænsning af hvilke oplysninger der må registreres, f.eks. hvilke oplysninger der opfylder formålet
- en fastlæggelse af hvordan de registrerede oplysninger må anvendes, f.eks. at oplysningerne kun må benyttes til nærmere beskrevne opgaver
- en regulering af videregivelse af oplysningerne, f.eks. at oplysningerne kun må videregives i

udtrykkelig beskrevne tilfælde

- et krav om sletning af oplysninger, f.eks. at oplysninger skal slettes efter en bestemt kort tidsperiode.

Det er blevet påpeget, at der kan blive tale om meget forskellige forhold, som det kan være vanskeligt at regulere alene ved lovgivning. Dertil kommer, at det i praksis vil være meget vanskeligt at kontrollere om reguleringen faktisk overholdes. Det er i den forbindelse foreslået, at man supplerer lovgivning med en adfærdskodeks, som er udarbejdet af brancheforeninger, forbrugerorganisationer og lignende i samarbejde med Registertilsynet. Med denne fremgangsmåde kan man tænke sig at reglerne har bedre forståelse og accept hos de virksomheder, som skal følge dem. [24]

EU-direktiv

Kommissionen fremlagde i september 1990 et forslag til direktiv om databeskyttelse. Direktivet har siden været behandlet i Parlamentet, og et ændret forslag fra Kommissionen har været gennem en langvarig behandling på embedsmandsplan. Først i februar 1995 kunne Ministerrådet vedtage en fælles holdning [25]. Den skal nu behandles af Parlamentet, og man kan ikke (maj 1995) vide i hvilket omfang forslaget bliver ændret før det evt. endelig vedtages.

Direktivet formulerer en række generelle principper for databeskyttelsen, som det enkelte medlemsland kan supplere. I art. 27 tilskyndes til udarbejdelse af adfærdskodekser for de forskellige sektorer. En adfærdskodeks kan også udarbejdes som en EF-kodeks.

Der rejser sig det spørgsmål, om reguleringen reelt vil blive ensartet på det konkrete niveau. Der er en mulighed for at det ikke sker, og at virksomhederne derfor kan flytte sig til det mest gunstige land. Som konsekvens heraf kan man i stedet forudse, at det enkelte medlemsland reelt må anvende direktivets minimumsniveau.

I relation til elektroniske spor må der derfor peges på vigtigheden af at det generelle direktiv udfyldes med en specifik regulering for relevante sektorer. Det kan ske ved at databeskyttelses-regulering indarbejdes i direktiver for en sektoren eller ved udarbejdelse de nævnte adfærdskodeks'er. Ændringer i direktivet om digitale telenet (omtalt i afsnit 4.1) giver anledning til at advare mod, at nærhedsprincippet anvendes på en måde, der reelt fører til en udhuling af databeskyttelsen.

I dansk lovgivning findes, som omtalt, en særlig regulering af betydning for elektroniske spor i lov om private registres særbestemmelser - f.eks. for registrering af telefonnumre og for videregivelse til markedsføringsformål -, og i betalingskortloven. Der må vises særlig opmærksomhed for at sikre at disse bestemmelser kan opretholdes.

6. Noter

1.Peter Blume: Personregistrering (1992) s. 214

Peter Blume: Persondatabeskyttelse i den private sektor (1995) afsnit 6: Elektroniske spor.

Ingvild Mestad: Elektroniske spor (CompLex 3/86) s. 1ff

2.Lov om private registre m.v. Lovbekendtgørelse nr. 622 af 2. oktober 1987.

3.DANMØNT Nyhedsbrev nr. 19 maj 1995.

4.Jean-Paul Boly et al: The ESPRIT Project CAFE (1994).

5.D. Chaum: Achieving Electronic Privacy (Scientific American august 1992) s. 76-81

6.Lov om betalingskort. Bekendtgørelse nr. 464 af 15. juni 1992 og ændringer i lov nr. 426 af 1. juni 1994.

7.Betænkning 1255: Elektronisk betalingsformidling uden betalingskort (1993) s. 61.

8.Keld Nielsen: Datasikkerhed i det offentlig net. Dansk Sikkerhedskonference 1993.

9.Denne tjeneste udbydes endnu ikke af TeleDanmark.

10.Der kan henvises til en norsk afhandling som behandler spørgsmålet: Ingvild Hanssen-Bauer: Personvern i digitale telenett (CompLex 3/93).

11.Forslag til Rådets direktiv om beskyttelse af personoplysninger og kommunikationshemmeligheden i forbindelse med offentlige digitale telenet, herunder det tjenesteintegrerede digitalnet (ISDN) og offentlige digitale mobilnet. Kom(90) 314 (syn 288).

12.Forslag til Europa-parlamentets og Rådets Direktiv: om beskyttelse af personoplysninger og kommunikationshemmeligheden i forbindelse med digitale telenet, herunder det tjenesteintegrerede digitalnet (ISDN) og digitale mobilnet. KOM (94) 128 endelig udg. (COD 288), den 13.06.1994.

13.Lov om offentlige myndigheders registre. Bekendtgørelse nr. 654 af 20. september 1991

14.Justitsministeriets bekendtgørelse om undtagelse af visse typer af offentlige edb-registre fra forskriftskrav m.v. nr. 872 af 17. december 1991.

15.Jan Kildebogaard: Hvad er trafikinformatik? (vdlnyt oktober 1991) s. 2.

16.Bangemann rapporten: Europa og det globale informationssamfund (1994).

17.Forskningsministeriet: Fra vision til handling. Info-samfundet år 2000 (1995).

18.TeknologiNævnet: På vej mod intelligent trafik. Slutdokument og ekspertoplæg fra konsensuskonferencen 28.-31. oktober 1994 (TeknologiNævnets rapporter 1995/1) s. 19.

19.Gitte Meyer: Store Mor (1992) s. 72-75 omtaler et forslag, der blev fremlagt i en rapport fra Norsk Regnecentral.

20.William E. Halal: Informations-teknologirevolutionen (Fremtidsorientering 3/1993) s. 38.

21.Anders Henten, Flemming Nielsen, Knud Erik Skouby: Forbrugerne og telepolitikken (Nord 1992:40) s. 110f.

22.David Chaum: Security without Identification: Transaction Systems to make Big Brother Obsolete. (Communication of the ACM october 1985 nr. 10 vol. 28).

23.Denne konklusion følger forslag fra TeknologiNævnets registergruppe i rapporten: Hvem ved hvad og bør de det? (1993).

24.Peter Blume: Persondatabeskyttelse i den private sektor (1995) s. 91 og 139f.

25.EU Ministerrådet: Fælles holdning nr. 12003/3/94 fastlagt af rådet den 3. februar 1995 med henblik på vedtagelse af Europa-Parlamentets og Rådets direktiv94/ /EF om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger.

22.12.97 Teknologirådet tekno@tekno.dk