Nordisk Ministerråd

Store Strandstræde 18
DK-1255 København K

Telefon 33 96 02 00
Telefax 33 96 02 02

nmr@norden.org

www.norden.org

Deloitte
Statsautoriseret Revisionsaktieselskab
CVR-nr. 24 21 37 14

Weidekampsgade 6
Postboks 1600
0900 København C

Telefon 36 10 20 30
Telefax 36 10 20 40

www.deloitte.dk

It-privacy
- en forudsætning eller en forhindring for borgeren i Norden?

2. december 2005

norden
Nordisk Ministerråd

Deloitte.
Medlem af
Deloitte Touche Tohmatsu

Deloitte

It-privacy
En forudsætning eller en forhindring for borgeren i Norden

TemaNord 2005:590

ISBN 92-893-1258-0

Omslag: Deloitte
Layout: Publikationsenheden, NMR
Omslagsfoto:
Flere publikationer på www.norden.org/publikationer

Nordisk Ministerråd
Store Strandstræde 18
1255 København K

Telefon (+45) 3396 0200
Fax (+45) 3396 0202

Nordisk Råd
Store Strandstræde 18
1255 København K

Telefon (+45) 3396 0400
Fax (+45) 3311 1870

www.norden.org

Udarbejdet for Nordisk Ministerråd af:

Deloitte
Stasautoriseret Revisionsaktieselskab
Weidekampsgade 6
Postboks 1600
0900 København C

Telefon (+45) 36 10 20 30
Fax (+45) 36 10 20 40

www.deloitte.dk

Det nordiske samarbejde

Det nordiske samarbejde er et af de ældste og mest omfattende regionale samarbejder i verden. Det omfatter Danmark, Finland, Island, Norge og Sverige samt Færøerne, Grønland og Åland. Samarbejdet styrker samhørigheden mellem de nordiske lande med respekt for de nationale forskelle og ligheder. Det øger mulighederne for at hævde Nordens interesser i omverdenen og fremme det gode naboskab.

Samarbejdet blev formaliseret i 1952 med *Nordisk Råds* oprettelse som forum for parlamentarikerne og regeringerne i de nordiske lande. I 1962 underskrev de nordiske lande Helsingforsaftalen, som siden har været den grundlæggende ramme for det nordiske samarbejde. I 1971 blev *Nordisk Ministerråd* oprettet som det formelle forum til at varetage samarbejdet mellem de nordiske regeringer og de politiske ledelser i de selvstyrende områder, Færøerne, Grønland og Åland.

Indholdsfortegnelse

Side

Bilagsrapporter

1. Introduktion

Embedsmandskomitéen for it-politik (EK-IT) har bestilt en opgave om analyse af ”it-privacy-området” hos Deloitte.

It-privacy – privatlivets fred – eller beskyttelse af persondata har aldrig tidligere været så aktuelt, som det er i denne tid, hvor ny teknologi vinder frem hurtigere, end man kan nå at forstå rækkevidden af mulighederne og truslerne for borgerne i relation til bevarelse af sin anonymitet og privatlivets fred.

Samtidig er der en stigende samfundsinteresse i automatisk at opsamle generel information med sigte på opklaring af eventuel kriminalitet af såvel national som international karakter.

I denne kontekst opstår en lang række dilemmaer i relation til, i hvilken udstrækning privatlivets fred må tilsidesættes i bekæmpelsen af kriminalitet og terror, samt i hvilken udstrækning overvågningen har den tilsigtede effekt.

Nærværende rapport beskriver Deloittes svar på de opgaver, som er blevet stillet os:

1. **Komparativ analyse** af de nordiske landes lovgivning om databeskyttelse
    - Sammenholdelse af databeskyttelseslovgivningen i de nordiske lande
    - Sammenholdelse af lovgivning omkring logning af elektroniske spor
    - Sammenholdelse af nordisk lovgivning på området med EU-reglerne
    - Udarbejdelse af notat med skema til sammenligning af lovgivningen
2. **Kortlægning** af tilgængelige privatlivsfremmende/privatlivstruende teknologier:
    - Identifikation og opdeling af teknologier i fremmende og truende
    - Kort beskrivelse af teknologiens formål, egenskab og mulighed/trussel
    - Udarbejdelse af notat med skema i overbliksform
3. **Vurdering** af, hvorledes de tilgængelige privatlivsfremmende/privatlivstruende teknologier forholder sig til krav og målsætning i persondatabeskyttelsesloven og logning af elektronisk spor:
    - De fælles krav og målsætninger fra de nordiske persondatabeskyttelseslove opstilles
    - De enkelte krav vurderes i forhold til hver enkelt teknologi kortlagt i opgave 2
    - Udarbejdelse af notat med konklusion samt skema til overblik

4. Kortlægning af de nordiske landes tiltag imod **spam** - en vurdering af spams betydning for privacy-området - og identifikation af mulige nye initiativer til bekæmpelse af spam:

   - Indsamling af viden om nordiske landes tiltag omkring bekæmpelse af spam ved udsendelse af spørgeskema
   - Opstilling af de enkelte landes tiltag i overskuelig form
   - Beskrivelse af mulige nye initiativer til bekæmpelse af spam pr. land med indikation af fælles tiltag
   - Vurdering af spams betydning for privacy-området – nu og i fremtiden
   - Udarbejdelse af et samlet notat, der beskriver tiltag, betydning og initiativer omkring spam

Vores arbejde er sammenfattet i nærværende rapport, der kan danne grundlag for debat og beslutning. Rapporten beskriver i en problematiserende og debatterende form de udfordringer og dilemmaer, som er fremkommet i forbindelse med løsning af opgaven.

Metode og afgrænsning

Rapportens primære formål er at give et input til debatten omkring privacy i Norden. Det har ikke været vores intention at give et fuldstændigt billede af de problemer og dilemmaer, der vil kunne identificeres i relation til privacy.

Ud fra den stillede opgave, de gennemførte analyser samt de resultater vi er kommet frem til, har vi, ud fra vores professionelle skøn og i samråd med projektgruppen under Videnskabsministeriet, udvalgt de dilemmaer, som præsenteres i rapporten. Vi har løst opgaven ved indsamling af forskellig information gennem tilgængeligt materiale på Internettet, afholdelse af møder og udsendelse af spørgeskemaer, samt anvendt vores erfaring fra arbejdet med it-sikkerhed hos private og offentlige virksomheder.

Rapportens formål er således ikke at komme med de detaljerede løsninger på de opstillede dilemmaer eller politiske udfordringer, da dette ligger uden for opgavens kommissorium. Et sådan arbejde kræver efter vores vurdering en mere detaljeret undersøgelse med henblik på at afdække løsningens samlede effekt ud fra en vurdering af fordele og ulemper i relation til målgruppen og anvendelsen, samt en skønsmæssig samfundsøkonomisk konsekvensberegning. Vi har dog i forbindelse med sammenfatningen opstillet nogle overordnede og generelle værktøjer i relation til udvalgte politiske udfordringer. Disse er alene tænkt som inspiration i debatten, og er ikke udtryk for en udtømmende liste af løsninger.

I hver delrapport er der for de enkelte opgaver givet en mere uddybende metodebeskrivelse og afgrænsning.

Læsevejledning

Nærværende rapport består af følgende delelementer:

1. **Sammenfatning.** Dette afsnit er en sammenfatning af rapportens primære konklusioner og dilemmaer.
2. **En rejse fra land til land – blandt privacy-dilemmaer**. Dette er en illustration af de privacy-dilemmaer, som en direktør i en opdigtet historie (men ikke langt fra virkeligheden) eventuelt vil komme ud for på en rejse fra København til Göteborg.
3. **Scenen sættes – problematisering over privacy.** Dette er en problematisering af emnet privacy formuleret i en blanding mellem spørgsmål og fakta med det formål indledningsvis at illustrere nogle af de vigtigste emner, som man bør være opmærksomme på i debatten om privacy.
4. **Potentielle privacy-dilemmaer til debat.** I dette afsnit sammenfattes privacy-dilemmaerne fra vores analyse i en problematiserende og debatterende form ud fra vores analysemodel, som har dannet ramme omkring vores arbejde.
5. **Bilagsrapporter.** Afslutningsvis er alle delopgaver særskilt og mere deltaljeret afrapporteret i fire delrapporter.

2. Sammenfatning

Som grundlag for denne hovedrapport har vi gennemført fire delopgaver, som har omfattet:
1. Sammenlignende analyse af de nordiske landes lovgivning omkring persondatabeskyttelse.
2. Kortlægning af potentielt privatlivsfremmende og privatlivstruende teknologier.
3. Vurdering af om teknologierne kan understøtte kravene i databeskyttelses lovgivningen.
4. Kortlægning af de nordiske tiltag omkring spam.

Disse delrapporter er summeret sammen i denne hovedrapport, som er et oplæg til debat vedrørende it-privacy i Norden. Debatten omkring it-privacy – privatlivets fred – og beskyttelse af persondata har aldrig tidligere været så aktuel som nu. Vi er i en tid, hvor den ny teknologi vinder frem hurtigere end nogensinde før, og hvor anvendelsesformerne af teknologien fornyes og sammensmeltes på nye måder. Brug af nogle teknologier bærer i sig potentialer til at udgøre trusler for borgerne i relation til bevarelse af anonymitet og privatlivets fred. Men samtidig kan samme teknologier anvendes til bekæmpelse af kriminalitet, f.eks. gennem etablering af øget overvågning, logning og lignende. Omvendt kan privatlivsfremmende teknologier udnyttes til f.eks. sløring af kriminelle aktiviteter.

I denne kontekst opstår der en lang række dilemmaer i relation til, hvornår og i hvilken udstrækning privatlivets fred må tilsidesættes i bekæmpelsen af kriminalitet. Dertil kommer behovet for at vurdere effekten af tiltag som overvågning m.v., i forhold til den pris, samfundet må betale i form af at måtte give afkald på privatliv.

I Norden har vi et lovgrundlag, der udgør et godt og tilstrækkeligt fundament for beskyttelsen af privatlivets fred og persondata. Beskyttelsen findes bl.a. i personoplysningslovene. Da personoplysningslovene har fokus på anvendelsen af de data, som hører under lovene, og ikke på de teknologier, der anvendes, er lovens virkefelt dækkende både nu og i fremtiden på trods af teknologiernes hastige forandring. Lovene om persondatabeskyttelse varierer lidt blandt de nordiske lande, og der kan derfor være mindre forskelle i beskyttelsesniveauet. Dette vurderes dog ikke at have en væsentlig betydning for beskyttelsen af privatlivets fred, som det er defineret i dag.

Ved anvendelse af nye teknologier får vi nye muligheder for effektivt og fleksibelt at udvide vores muligheder for kommunikation og handel i dagligdagen. Men samtidigt bliver vi mere eller mindre tvunget til at afgive informationer om os selv og vores færden, ønsker og behov. Informationer, som vi indtil i dag har betragtet som grundlæggende for beskyttelsen af privatlivets fred. Derfor rejser der sig et spørgsmål om, hvorvidt det stadig er relevant at beskytte informationer på samme niveau og med samme metoder som tidligere. Og i hvor stor udstrækning ønsker borgerne denne beskyttelse?

Teknologierne kan sjældent udelukkende kategoriseres som enten privatlivsfremmende eller privatlivshæmmende. Det er anvendelsen af teknologierne og de muligheder, der stilles til rådighed for bru-

gerne, der afgør, om teknologien er potentielt fremmende eller hæmmende for privatlivets fred. Dette rejser dilemmaet om niveauet for privacy til beskyttelse af borgernes rettigheder i forhold til nationalstatens og det globale samfunds ønske om beskyttelse og opklaring af kriminalitet m.v.

Nationalstaterne har en ikke ubetydelig rolle i privacy-debatten, primært ved etablering og anvendelse af forskellige styringsmidler som f.eks. lovgivning til sikring af privacy. Den elektroniske information, som ønskes overvåget/logget, passerer ofte internationale landegrænser, som således påvirker betydningen af national lovgivning. Såvel privacy-fremmende som privacy-hæmmende teknologier udvikles typisk uden for de enkelte staters kontrol f.eks. af forskere og studerende i internationale åbne miljøer. At lovgive mod sådanne teknologier har således kun ringe effekt.

Teknologien og dens anvendelsesmuligheder er kompleks, og i mange sammenhænge bliver det uforståeligt for borgerne. Nationalstaterne har derfor en vigtig rolle i at fremme privacy for borgerne ved f.eks. at informere og understøtte forståelsen af nødvendigheden af at anvende privatlivsfremmende teknologier på en måde, så borgernes privatlivsfred stadig sikres. Samtidig må borgerne have tillid til, at lovgiver kan overskue konsekvenser og muligheder i anvendelsen af teknologierne og i lyset heraf iværksætte initiativer, der beskytter data omkring borgernes privatliv på bedst mulig måde. Spørgsmålet er, om staten skal føre et proaktivt tilsyn med virksomheders overholdelse af privacy-lovene i de Nordiske lande. Og om det er realistisk i lyset af den stigende globaliserings betydning herfor.

I sidste ende har borgerne dog selv et ansvar for at anvende de løsninger og muligheder, som er til rådighed. Der findes i dag muligheder for at sikre privacy, når man f.eks. anvender Internettet. Disse muligheder er dog i dag ikke almindeligt udbredt, og der synes ikke iværksat globale initiativer, der understøtter dem. Der findes dog en række private initiativer, som har skabt mulighed for bl.a. krypteret IP-telefoni, anonymizer-programmer og simple krypteringsprodukter til download på nettet, men det er ikke nationale initiativer. Der er dog i Norden igangsat initiativer inden for spam og kryptering.

I de nordiske lande har vi lovgivning omkring persondata, mens debatten omhandler begrebet privacy. Det er vores vurdering, at privacy omfatter mere end persondatalovens rammer. Det er derfor nødvendigt at udvide debatten omkring øget privatlivsfremmende og privatlivshæmmende tiltag som f.eks. overvågning med en åben og grundlæggende fastlæggelse af, hvad vi i dag forstår ved privatlivets fred og privacy, samt hvad teknologien giver af muligheder. Denne debat bør tages i såvel de enkelte nationer som på tværs af landegrænser i nordiske, europæiske og globale fællesskaber. Teknologiernes anvendelse viser med al tydelighed, at data flyttes over grænserne og bliver vanskeligere for de enkelte lande at kontrollere. Der er derfor behov for en styrkelse af det globale samarbejde på privacy-området.

Undersøgelsen har vist, at et af de grundlæggende dilemmaer er at finde en tilstrækkelig balance mellem sikring af borgernes privacy og nationalstatens interesse, herunder de globale interesser. Derfor rejser der sig en række spørgsmål som:

- Hvor meget overvågning og kontrol ønsker borgerne for at kunne opnå en større reel sikkerhed mod kriminalitet m.m. på bekostning af privacy?
- Er det acceptabelt, at de kriminelle ikke altid forhindres i deres aktivitet ved øget kontrol og overvågning, når der er fri adgang til potentielt privatlivsfremmede teknologier?
- Hvordan fremmes borgernes mulighed for at sikre privatlivets fred ved benyttelse af potentielt privatlivsfremmende teknologier?
- Hvilke andre styringsmidler end lovgivning kan tages i anvendelse for at sikre privacy data, når disse i stigende grad i takt med globaliseringen flyder over landegrænser - og dermed på tværs af staternes lovgivning?

3. En rejse fra land til land – blandt privacy-dilemmaer

Nedenstående oversigtsbillede og historie viser et eksempel på en 2 dages forretningsrejse for en dansk koncerndirektør, der har et forretningsmøde i Göteborg. Under koncerndirektørens rejse flyver han til Göteborg, spiser ude i byen om aftenen, overnatter på hotel, har et forretningsmøde og holder en åben tale hos en virksomhed i Göteborg, hvorefter han flyver tilbage til Danmark. Direktøren har desuden sin sekretær med, som skal assistere ham undervejs på hans rejse.

Hensigten med dette eksempel er at give et indblik i al den information, der lagres om vedkommende i den periode. På oversigtsbilledet (figur 1) ses de forskellige punkter, hvor information lagres om koncerndirektøren, og disse punkter er beskrevet.

I løbet af rejsen opsamles og registreres flere typer af informationer omkring koncerndirektøren:

- Persondata, som er følsomme oplysninger, der kan misbruges til f.eks. identitetstyveri ved aflytning af bl.a. pinkoder ved brug af kreditkort.
- Bevægelsesdata, der fortæller noget om, hvor koncerndirektøren har været eller er lige nu, f.eks. oplysninger omkring adgang til begrænsede områder eller bestilling af taxa.
- Overvågningsdata, der indsamles via kameraer og anden overvågnings- og aflytningsudstyr, f.eks. i lufthavne.
- Adfærdsdata, der er oplysninger omkring personens adfærd, f.eks. indkøb af forskellig slags.

Herefter følger en kort opsummering over samtlige antal oplysninger, der er opsamlet og registreret i forbindelse med koncerndirektørens rejse.

Privatlivshæmmende potentialer	**Antal af dataregistreringer**
Persondata	18
Bevægelsesdata	21
Overvågningsdata	7
Adfærdsdata	5
I alt	**51**

Dette leder bl.a. til potentielle privacy-dilemmaer omkring personoplysninger, retten til at bevæge sig frit og anonymt – og samtidig den tryghed og effekt, som overvågning giver, da det i statens og samfundet interesse giver mulighed for at identificere eventuel uønsket adfærd.

I modsætning til ovenstående dataindsamling er der i casen også medtaget eksempler på privatlivsfremmende teknologier (privacy enhancing tecnologies, PET), som sikrer en anonymitet eller høj sikkerhed, når data udveksles. Disse kan læses ud fra den korrupte sekretærs handlinger igennem casen.

Sekretæren har en noget anden dagsorden, end den direktøren kender til. Hun er nemlig hyret af et bureau til at indhente fortrolige oplysninger om direktørens firma, som derefter viderebringes til tredje mand. Hvad disse oplysninger skal bruges til er ukendt, men sekretæren benytter den nyeste teknologi til at optræde så anonymt som muligt, så ingen får færden af hendes korrupte og hemmelige dagsorden.

Herefter følger en kort opsummering over de punkter, hvor oplysninger er anonymiseret, og er derfor ikke genkendelig i den registrerede form:

Privatlivsfremmende potentialer	**Antal gange anvendt**
Benyttelse af VPN-tunnel	1
Forsendelse af mail m. digital signatur	2
Benyttelse af anonymiseringsværktøj til sløring af IP-adresse og forsendelse af mail	2
Benyttelse af mobiltelefon med anonymt taletidskort	1
I alt	**6**

Følgende illustration viser koncerndirektørens rejse punkt for punkt:

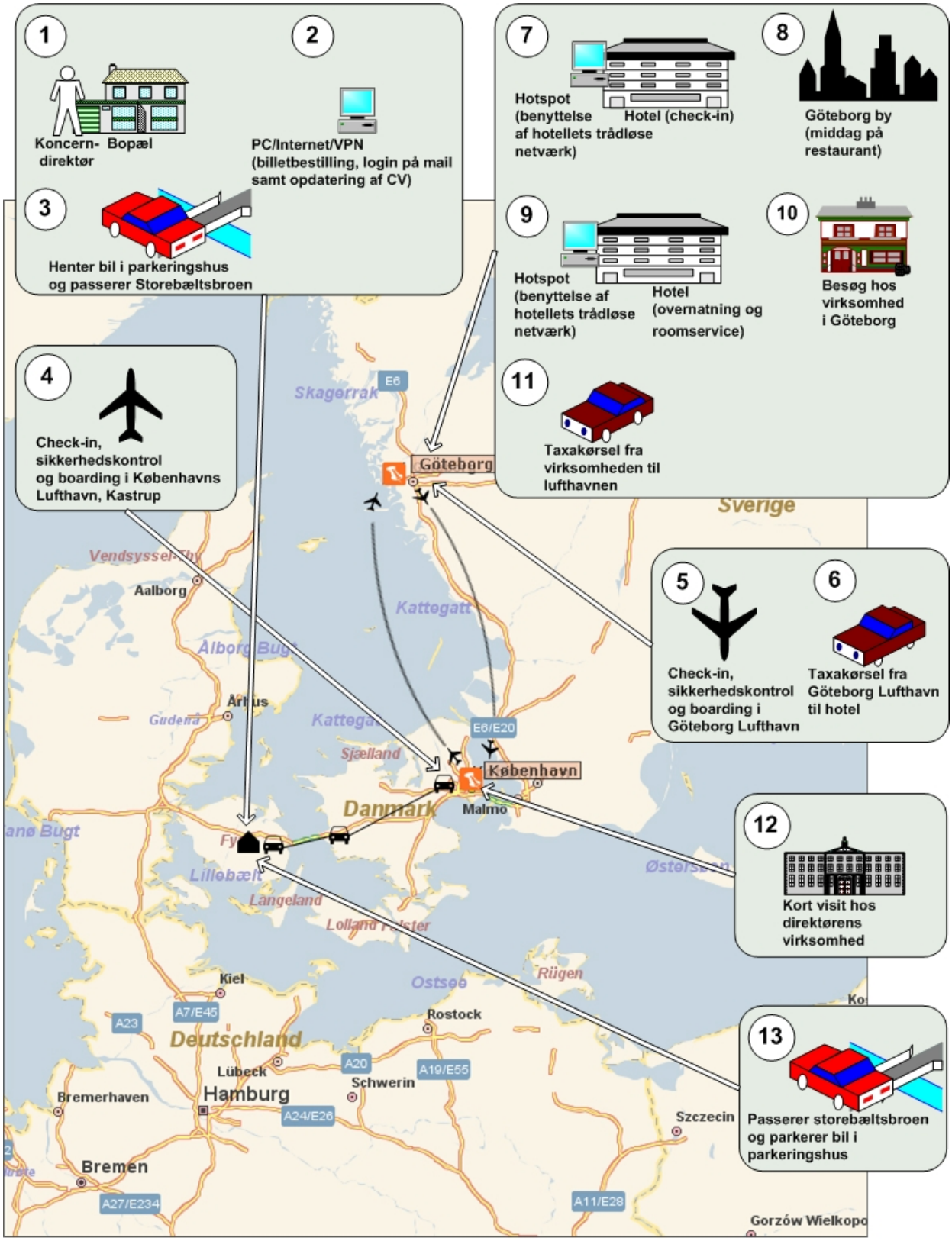


Fig. 1 - Oversigtsbillede over de punkter, hvor dataindsamling finder sted under koncerndirektørens rejse.

Koncerndirektørens rejse punkt for punkt

Nedenfor ses en tabel opdelt i tre kolonner. Den første kolonne viser, hvem der har ansvar for de data, der bliver registreret i forbindelse med koncerndirektørens rejse og færden. Den anden kolonne skildrer koncerndirektørens rejse punkt for punkt, og den sidste kolonne nævner de potentielle privacy-dilemmaer, der er forbundet med den informationssamling, der finder sted.

Ansvar for data (datatype)	Punkt	Privacy-dilemmaer
Flyselskab (persondata)	**1 og 2.** Koncerndirektøren har på forhånd bestilt sin flybillet over nettet, hvor navn og adresse skal oplyses for at kunne købe billetten, da der skal oprettes en brugerkonto hos flyselskabet.	***1.1 Hurtig betjening ved check-in på bekostning af mulighed for misbrug af personlige oplysninger samt phishing.***
ISP[1] (bevægelsesdata og persondata)	Inden koncerndirektøren kører til lufthavnen tjekker han sin mail ved at logge ind på sin firmamail igennem en VPN-tunnel.[2] Han er derved beskyttet af kryptering og virksomhedens firewall. Han besøger desuden et online politisk debatforum, hvor han opdaterer sin profil, som er oprettet på forummet. ..... Flyselskabet, hvorigennem billetten er købt, har nu registreret oplysninger om navn, adresse, nationalitet og rejseaktivitet samt login. Dette er gemt i en database, som flyselskabet administrerer. Firmaet har nu registreret logintidspunktet og det brugernavn, der er blevet logget ind med via VPN. Debatforummet har registreret ændringer af koncerndirektørens profil. ISP (Internet Service Provideren) har registreret IP- og MAC-adresse[3] samt besøgte websider, tidspunkt mv.	***2.1 Fleksibel adgang til Internettet på bekostning af risiko for opsnapning af personlige oplysninger uden om VPN (afhængig af, om VPN-tunnelen omfatter browseren eller kun mailklienten).***
Parkeringshuset (bevægelses- og overvågningsdata)	**3.** Koncerndirektøren har sin bil parkeret i et parkeringshus, hvortil adgang opnås med elektronisk nøgle og dertilhørende password. Der er desuden videoovervågning i parkeringshuset.	***3.1 Sikker parkering og færden kontra misbrug af oplysninger om adgangstidspunkt til parkeringshus, der giver oplysninger om, hvornår bilen er i brug eller personen ikke er hjemme.***
Storebæltsbroen (bevægelsesdata)	Koncerndirektøren bor på Fyn, så han passerer Storebæltsbroen, hvortil han har brobizz. Brobizz-senderen, som han har installeret i sin bil, giver ham adgang over broen.	***3.2 Bekvem og hurtig passage med sender kontra misbrug af oplysninger om adgangstidspunkt til Storebæltsbroen.***

[1] Internet Service Provider

[2] Et virtuelt privat netværk (virtual private network), som danner en sikker tunnel, hvor data bliver krypteret.

[3] (Media Access Control). En unik kode, som de fleste former for netværks-devices er tildelt. Bl.a. netværkskort.

Ansvar for data (datatype)	Punkt	Privacy-dilemmaer
	Oplysninger om ankomsttidspunkt til parkeringshuset er nu gemt i database, som parkeringshuset administrerer. Videoovervågning er gemt i arkiv. Oplysning om færdsel over broen er nu registreret.	
Parkeringshus (bevægelses- og overvågningsdata)	**4.** Koncerndirektøren ankommer til Københavns Lufthavn, Kastrup. Koncerndirektøren parkerer sin bil i et videoovervåget parkeringshus.	***4.1 Sikker parkering og færden kontra misbrug af oplysninger om adgangstidspunkt til parkeringshus, der giver oplysninger om, hvornår bilen er i brug eller personen ikke er hjemme.***
Lufthavn (overvågning)	Koncerndirektøren tjekker ind ved check-in skranken. Han viser sit pas og sin billet samt afleverer bagagen, hvilket overvåges via videokamera. Han mødes med sin sekretær, som skal følge ham på hans rejse til Göteborg.	***4.2 Identitetssikkerhed er at personen er den han udgiver sig for på bekostning af den enkeltes anonyme bevægelsesfrihed.***
Politiet (person- og bevægelsesdata)	Koncerndirektøren går igennem sikkerhedskontrollen, hvor hans taske også bliver scannet for våben og andet. I sikkerhedskontrollen bliver han identificeret ved hjælp af ansigtsgenkendelse, der benytter 3D data, som verificering af, at koncerndirektøren er identisk med data, som er nedskrevet og opbevaret elektronisk i passet. Verificeringen af data sammenholdes også med eventuelle blacklistede og efterlyste personer.	***4.3.1 Høj sikkerhed ved ansigtsgenkendelse, der sikrer, at personen er identisk med personen i passet på bekostning af privacy for den enkelte (undtagelser for PET/FET).*** ***4.3.2. Oplysninger om personers færden ved efterlysninger kontra retten til frit at forlade landet uden oplysninger til de nærmeste.***
Bank, betalingsmodtager (persondata)	Koncerndirektøren køber en kop kaffe og en avis med sit kreditkort, mens han venter på at blive boardet.	***4.4 Bekvem betalingsform versus tyveri af "kontanter", men afgiver information om køb.***
Flyselskab (adfærdsdata)	Koncerndirektøren køber et par flasker spiritus til eget forbrug. Køb af alkohol og cigaretter, hvor koncerndirektøren viser sit boardingcard, hvorpå købet registreres hos lufthavnsvæsnet. Hans køb registreres i lufthavnen til senere service over for kunden, hvor tilbud sendes via sms næste gang han kommer i lufthavnen, baseret på hans købsprofil.	***4.5 Toldsupport til sikring af, at afgiftsregler overholdes i modsætning til oplysninger om koncerndirektørens adfærd.***
Lufthavn (bevægelsesdata)	Koncerndirektøren boarder flyet og boardingcard bliver indscannet.	***4.6 Sikkerhed om bord på flyet versus individets***

Ansvar for data (datatype)	Punkt	Privacy-dilemmaer
Lufthavn (overvågning)	I lufthavnen er der videoovervågning de fleste steder. ..... Oplysninger om check-in tidspunkt og boarding info er nu lagret i flyselskabets database. Betaling af kaffe og avis samt køb af spiritus med kreditkort er registreret hos de transaktionsansvarlige[4]. Videoovervågning er gemt i arkiv. Verificering af ansigtsgenkendelse og sammenholdelse er gemt i lufthavnens biometriske database, som værende godkendt på udrejsetidspunktet.	***bevægelsesfrihed.*** ***4.7 Identitetssikkerhed at personen er den han udgiver sig for på bekostning af den enkeltes anonyme bevægelsesfrihed.***
Lufthavn (overvågning) ***Teleudbyder (persondata, adfærdsdata, og bevægelsesdata)*** ***Indløser, bank, betalingsmodtager (persondata)***	**5.** Koncerndirektøren er nu ankommet til Göteborg Lufthavn, hvor der også er videoovervågning over det meste af lufthavnen. Koncerndirektøren bestiller en taxa til sit hotel via sin mobiltelefon. Koncerndirektøren betaler med sit kreditkort i taxaen. ..... Videoovervågning er gemt i arkiv. Brug af mobiltelefon er registreret hos teleudbyder. Oplysninger om brug af kreditkort til betaling for taxatur er nu registreret hos de transaktionsansvarlige.	***5.1 Identitetssikkerhed at personen er den han udgiver sig for på bekostning af den enkeltes anonyme bevægelsesfrihed.*** ***5.2 Bevægelsesfrihed og bekvem transport på bekostning af risiko for bevægelsesoplysninger i de forkerte hænder.*** ***5.3 Bekvem betalingsform versus tyveri af "kontanter", men afgiver information om køb.***
Hotellet (persondata og adfærdsdata) ***ISP (persondata)***	**6.** Koncerndirektøren ankommer til hotellet i Göteborg by, hvor han skal overnatte. Koncerndirektøren tjekker ind hos conciergen og modtager en nøgle til værelset. Da koncerndirektøren er en prominent gæst, har hotellet noteret få oplysninger ned om koncerndirektøren, såsom ønsker om indretning og værelsestype, ønsker til roomservice, ankomst- og afgangstidspunkt. Koncerndirektøren fortæller ligeledes conciergen om hans ærinde i Göteborg, som består i et møde og en åben tale hos en svensk virksomhed, og dette noteres også ned. Udover dette bestiller koncerndirektøren adgang til hotellets trådløse netværk, som han benytter til at tjekke mail med efter ankomst til	***6.1 Økonomisk sikkerhed for hotellet og hotellets ønske om gensalg på bekostning af risiko for spam og videregivelse af adfærdsdata.*** ***6.2 Mobil arbejdsplads kontra risiko for blandt***

[4] **Forbrugsoplysninger, mv.**
Ved brug af kreditkort registreres kortets nummer, det samlede transaktionsbeløb, dato for brug af kreditkortet og hvor kreditkortet har været benyttet. Betalingsmodtager videresender disse oplysninger til banken via PBS. Oplysningerne opbevares hos betalingsmodtager, PBS og hos banken og anvendes i bogføringen, ved fakturering/kontoudtog (herunder elektronisk kontoudtog og eventuel adgang for kortindehaver til at se sit forbrug via Internettet) og eventuel senere fejlretning.

Ansvar for data (datatype)	Punkt	Privacy-dilemmaer
	hotelværelset. Der er ligeledes bestilt internetadgang til sekretæren, som også er boende på hotellet.	***andet phishing, vira, videregivelse af oplysninger om hvor personen befinder sig.***
Hotellet (adfærdsdata)	Koncerndirektøren benytter hotellets minibar til at forsyne sig med drikkevarer.	***6.3 Bekvem service versus registrering af adfærdsdata.***
Udbyder af signatur (persondata)	På hotelværelset skriver koncerndirektøren en fortrolig mail til sin sekretær, som han påfører en digital signatur, for at sikre sig, at indholdet er konfidentielt og intakt når det når frem.	***6.4.1 Registrering for at verificere at afsender og modtager er korrekte, mens bedragere går fri.*** ***6.4.2 Administrationen af digital signatur er outsourcing af oplysninger til private, i modsætning til opbevaring hos personnummerregistre under statens kontrol.***
Udbyder af taletidskort (anonym persondata)	Sekretæren modtager den krypterede mail fra koncerndirektøren, som indeholder fortrolige oplysninger om firmaet. Sekretæren kontakter i den forbindelse bureauet, som har hyret hende, da hun vil sende de fortrolige oplysninger videre til tredjemand. Hun vil nu forhandle betaling for de fortrolige informationer, som hun ligger inde med og benytter derfor sin ekstratelefon, som er købt kontant hos en privat sælger, til at kontakte bureauet med. Hun isætter et SIM-kort med dertilhørende taletid, som også er købt kontant i en kiosk. Hun benytter telefonindstillingen "skjul nummer", inden hun ringer. Sekretærens bærbare computer er beskyttet med harddiskpassword, og al fortroligt materiale er kodet og gemt som steganografi (usynligt støj på computeren, som kun kan ses med bestemte programmer. Steganografi gør det f.eks. muligt at skjule data som et almindeligt JPEG-billede). ..... Oplysninger om ankomsttidspunkt, antal personer der tjekker ind, oplysninger om personlige ønsker til indretning af værelse og roomservice samt ærinde i Göteborg, er nu noteret i hotellets gæstedatabase. Opkoblingstid på det trådløse netværk (herunder forbindelsens IP-adresse, MAC-adresse samt nettrafik) er registreret. Oplysninger om forsendelse af mail med digital signatur, er gemt hos ISP.	***6.5 Registrering af opkald foretaget med taletidskort. Det er ikke muligt at knytte en bruger til nummeret, der ringes fra, da taletidskortet sikrer brugeren anonymitet.***
Teleudbyder (bevægelsesdata)	**7.** Koncerndirektøren bestiller via hotellets værelsestelefon bord på en restaurant i Göteborg by. Koncerndirektøren og sekretæren spiser middag på restaurant i Göteborg.	***7.1 Økonomisk sikkerhed for hotellet og hotellets ønske om gensalg på bekostning af risiko for spam og videregivelse af adfærdsdata.***

Ansvar for data (datatype)	Punkt	Privacy-dilemmaer
Indløser, bank, betalingsmodtager (persondata)	Koncerndirektøren betaler regningen med sit kreditkort. ..... Oplysninger om brug af værelsestelefon, bordbestilling og køb af mad er nu registreret hos henholdsvis hotellets telefonudbyder, restaurantens bordbestillingsdatabase samt de ansvarlige for kreditkorttransaktioner.	***7.2 Bekvem betalingsform versus tyveri af "kontanter", men afgiver information om køb.***
Hotellet (bevægelsesdata) ***ISP (persondata)***	**8.** Efter middagen vender koncerndirektøren og sekretæren tilbage til hotellet. Hotellet registrerer ankomsttidspunktet for koncerndirektøren, ligesom adgangen til værelset med elektronisk nøgle registrerer ankomsttidspunkt. På hotelværelset benytter koncerndirektøren endnu engang hotellets trådløse netværk for at tjekke sin mail. Sekretæren sender desuden koncerndirektøren et par fortrolige mails vedr. mødet med den svenske virksomhed. Mails er sendt med digital signatur.	***8.1 Sikkerhed angående hvem der har adgang til værelserne, kontra overvågning af den enkeltes færden.*** ***8.2 Fleksibel adgang til Internettet på bekostning af risiko for opsnapning af personlige oplysninger uden om VPN (afhængig af, om VPN-tunnelen omfatter browseren eller kun mailklienten).*** ***8.3 Registrering for at verificere at afsender og modtager er korrekte, mens bedragere går fri.***
Udvikler (persondata) ***Pengeinstitut (persondata)***	Sekretæren benytter det trådløse netværk, men ønsker ikke at IP-adressen bliver logget. Derfor benytter sekretæren et webanonymiseringsværktøj, som er tilgængelig flere steder på Internettet. Eksempelvis Freenet (http://freenetproject.org). Dette værktøj usynliggør IP-adressen, så besøgte websider ikke kan aflæse adressen på den besøgende. Koncerndirektøren skal overføre penge til en anden konto og vil benytte sig af sin webbank. Han har sin elektroniske sikkerhedsnøgle med på en USB-stick, som giver ham adgang til webbank.	***8.4 Anonymisering af bevægelser på nettet kontra installation og registrering af software.*** ***8.5 Fleksibel bankløsning med risiko for tyveri af kontanter og personlig information via phising. m.m.***
Hotellet (adfærds- og bevægelsesdata)	Koncerndirektøren benytter desuden roomservice til at få bragt natmad og en enkelt drink op på værelset. ..... Oplysninger om ankomsttidspunkt til hotellet samt bestilling af room-	***8.6 Økonomisk sikkerhed for hotellet og hotellets ønske om gensalg på bekostning af risiko for spam og videregivelse af adfærdsdata.***

Ansvar for data (datatype)	Punkt	Privacy-dilemmaer
	service, er nu henholdsvis lagret i hotellets gæstedatabase samt hotellets roomservicedatabase. Opkoblingstid på det trådløse netværk (herunder forbindelsens IP-adresse, MAC-adresse samt nettrafik) er registreret. Benyttelse af webbank er registreret hos koncerndirektørens pengeinstitut.	
Hotellet indløser, bank, betalingsmodtager (person- og bevægelsesdata)	**9.** Efter en god nats søvn på hotellet skal koncerndirektøren deltage i et møde samt holde en åben tale hos en virksomhed i Göteborg. Koncerndirektøren tjekker ud af hotelværelset inden han drager videre og betaler hotelregningen med kreditkort.	***9.1 Ukompliceret betalingsform kontra risiko for misbrug af kortoplysninger.***
Virksomheden (bevægelsesdata)	Da koncerndirektøren ankommer til virksomheden bliver han registreret og godkendt som gæst i virksomhedens database over ankommende gæster, der skal have tilladelse til at komme ind, og får desuden udleveret en trådløs adgangsnøgle. Alt dette foregår i receptionen. I den trådløse adgangsnøgle findes en RFID chip. Ved hjælp af denne chip behøver koncerndirektøren blot at stille sig foran en dør og denne vil blive åbnet, da RFID chippen udsender trådløse signaler til modtagere opstillet ved døre.	***9.2 Sikkerhedsaspekt ved kontrol af hvem der bevæger sig rundt i bygningen versus hensyntagen til den enkeltes privacy.***
Medier (bevægelsesdata)	Ved sin ankomst bliver koncerndirektøren desuden interviewet af flere forskellige svenske aviser samt nogle få danske journalister, der har fulgt koncerndirektøren i hans rejse til Sverige. Der bliver også taget billeder af koncerndirektøren samt nedskrevet ord for ord, hvad han svarer på de stillede spørgsmål. Disse interviews bliver trykt og lagt online på flere avis websider, samt videooptagelserne bliver vist i dansk tv. Koncerndirektøren deltager i mødet samt holder sin tale hos virksomheden, som bliver set, optaget og filmet af svenske samt danske journalister.	***9.3 Hurtig videndeling i modsætning til opbevaring af data, herunder mistolkning af information.***
Virksomheden (bevægelsesdata)	Ved udgangen afleverer koncerndirektøren sit adgangskort tilbage til receptionisten, som registrerer hans afrejse samt aflevering af kort.	***9.4 Sikkerhedsaspekt ved kontrol af hvem der bevæger sig rundt i bygningen versus hensyntagen til den enkeltes privacy.***
Caféens ISP (persondata)	Sekretæren benytter sin frokostpause til at besøge en lokal café, hvor der er mulighed for gratis at benytte trådløse netværk. Hun bruger endvidere sit trådløse USB-netværkskort i stedet for computerens eget indbyggede. Netkortet er købt kontant, og er dermed en anonym MAC-adresse.	***9.5 Fleksibel adgang til Internettet på bekostning af risiko for opsnapning af personlige oplysninger.***
Udvikler (persondata)	For at være helt sikker benytter hun et anonymiseringsværktøj til at browse Internettet med. Således kan sekretærens web-browsing ikke spores til hendes geografiske position via caféens IP-adresse og heller ikke til hendes computers MAC-adresse.	***9.6 Anonymisering af bevægelser på nettet kontra installation og***

Ansvar for data (datatype)	Punkt	Privacy-dilemmaer
	Sekretæren vil nu sende de oplysninger, hun har samlet sammen om koncerndirektøren og hans firma. Hun benytter stærk kryptering på sine informationspakker (krypteringsværktøjet er open souce) og benytter Freenet til at sende sin anonyme e-mail med. ..... I forbindelse med hans møde og tale hos virksomheden i Göteborg, er følgende oplysninger blevet logget: ankomst og afrejse til virksomheden samt udlevering og aflevering af adgangskort, åbne interviewspørgsmål samt svar er nedskrevet af flere journalister, og der er desuden taget billeder af koncerndirektøren. Hans tale er filmet og set af flere mennesker, samt det er kommentarer og spørgsmål til talen nedskrevet af journalister, som senere bruger denne information både i trykte og online medier. Disse bliver gemt i en database, som hvert medie administrerer. Videooptagelser bliver gemt i arkiv. I forbindelse med hans afrejse fra hotellet, er hans afrejsetidspunkt samt oversigt over forbrug registeret i hotellets gæstedatabase, samt betaling med kreditkort registreret hos de transaktionsansvarlige.	***registrering af software.***
Indløser, bank, betalingsmodtager (person- og bevægelsesdata)	**10.** Koncerndirektøren tager en taxa til Göteborg Lufthavn. Koncerndirektøren betaler med sit kreditkort i taxaen. ..... Oplysninger om brug af kreditkort i forbindelse med betaling af taxatur, er nu gemt hos de transaktionsansvarlige.	***10.1 Bekvem betalingsform versus tyveri af "kontanter", men afgiver information om køb.***
Lufthavnen (persondata) ***Politiet (person- og bevægelsesdata)***	**11.** Koncerndirektøren ankommer til Göteborg Lufthavn. Koncerndirektøren tjekker ind ved check-in skranken. Han viser sit pas og sin billet samt afleverer bagagen. Koncerndirektøren går igennem sikkerhedskontrollen, hvor hans taske også bliver scannet for våben og andet. I sikkerhedskontrollen bliver han identificeret ved hjælp af ansigtsgenkendelse, der benytter 3D data, som verificering af, at koncerndirektøren er identisk med data, som er nedskrevet og opbevaret elektronisk i passet. Verificeringen af data sammenholdes også med en database indeholdende blacklistede og efterlyste personer, der er oplyst og videregivet til flyselskabet af politiet.	***11.1 Identitetssikkerhed at personen er den han udgiver sig for på bekostning af den enkeltes anonyme bevægelsesfrihed.*** ***11.2 Høj sikkerhed ved ansigtsgenkendelse, der sikrer, at personen er identisk med personen i passet på bekostning af privacy for den enkelte (undtagelser for PET/FET).*** ***11.2.3 Oplysninger om personers færden ved efterlysninger kontra retten til frit at forlade landet uden oplysninger til de nærmeste.***

Ansvar for data (datatype)	Punkt	Privacy-dilemmaer
Indløser, bank, betalingsmodtager (persondata)	Koncerndirektøren køber en dansk avis og et par drinks med sit kreditkort, mens han venter på at blive boardet.	***11.3 Bekvem betalingsform versus tyveri af "kontanter", men afgiver information om køb.***
Flyselskab (bevægelsesdata)	Koncerndirektøren boarder flyet og boardingcard bliver indscannet.	***11.4 Sikkerhed om bord på flyet versus individets bevægelsesfrihed.***
Lufthavnen (overvågning)	I lufthavnen er der videoovervågning de fleste steder. ..... Verificering af ansigtsgenkendelse og sammenholdelse, er gemt i lufthavnens biometriske database, som værende godkendt på udrejsetidspunktet. Oplysninger om check-in tidspunkt og boarding info er nu lagret i flyselskabets database. Betaling af kaffe og avis med kreditkort er registreret hos de transaktionsansvarlige. Videoovervågning er gemt.	***11.5 Identitetssikkerhed at personen er den han udgiver sig for på bekostning af den enkeltes anonyme bevægelsesfrihed.***
Lufthavnen parkeringshuset (bevægelsesdata)	**12.** Koncerndirektøren ankommer til Københavns Lufthavn, Kastrup og henter sin bil i parkeringshuset ved lufthavnen. I lufthavnen og i parkeringshuset er der videoovervågning. Koncerndirektøren kører direkte ind til sin virksomhed, hvor han skal aflevere nogle papirer fra besøget i Göteborg til en ansat.	***12.1 Sikker parkering og færden kontra misbrug af oplysninger om adgangstidspunkt til parkeringshus, der giver oplysninger om hvornår bilen er i brug eller personen ikke er hjemme.***
Koncerndirektørens virksomhed (bevægelsesdata)	I virksomheden er der fornyeligt blevet oprettet et personsøgningssystem, der fungerer via mobiltelefonen, som alle medarbejdere er udstyret med. I mobiltelefonen er en modtager, som giver signaler til en antenne om, hvor medarbejderne befinder sig i bygningen, og dette ses via et overbliksprogram, som er installeret på medarbejdernes pc'ere. Koncerndirektøren benytter dette program til at finde sin medarbejder, som ikke er på sin plads, og koncerndirektøren afleverer papirerne om mødet i Göteborg til den ansatte, da han finder hende igennem personsøgningssystemet.	***12.2 Effektiv personsøgning kontra overvågning af individets færden.***
Koncerndirektørens virksomhed (overvågningsdata)	Der er desuden videoovervågning de fleste steder i bygningen. ..... Oplysninger om bevægelser og opholdstid i virksomheden er registreret i en database ved hjælp af en sender indbygget i mobiltelefon. Videoovervågning er gemt i arkiv.	***12.3 Identitetssikkerhed at personen er den han udgiver sig for på bekostning af den enkeltes anonyme bevægelsesfrihed.***

Ansvar for data (datatype)	Punkt	Privacy-dilemmaer
	13. Koncerndirektøren kører fra virksomheden og hjem.	
Storebæltsbroen (bevægelsesdata)	Koncerndirektøren bor på Fyn, så han passerer Storebæltsbroen, hvortil han har brobizz. Brobizz-senderen, som han har installeret i sin bil, giver ham adgang over broen.	***13.1.1 Bekvem og hurtig passage med sender kontra misbrug af oplysninger om adgangstidspunkt til Storebæltsbroen.***
Parkeringshuset (bevægelsesdata)	Koncerndirektøren parkerer sin bil i parkeringshuset, hvortil adgang opnås med elektronisk nøgle og dertilhørende password. Der er desuden videoovervågning i parkeringshuset.	***13.1.2 Sikker parkering og færden kontra misbrug af oplysninger om adgangstidspunkt til parkeringshus, der giver oplysninger om hvornår bilen er i brug eller personen ikke er hjemme.***
	.....	
	Oplysning om færdsel over broen er nu registreret.	
	Oplysninger om ankomsttidspunkt til parkeringshuset er nu gemt i database, som parkeringshuset administrerer.	
	Videoovervågning er gemt i arkiv.	

Problemstillingen ved sammenkobling af data, der er lagret under rejsen

Som beskrevet i indledningen om denne case, var hensigten med dette eksempel at give et indblik i al den information, der lagres om vedkommende i denne periode. Det er vigtigt at forstå, hvad sammenkoblingen af den data, der er indsamlet, potentielt kan fortælle om koncerndirektørens adfærd. Som et led i forståelsen og som et eksempel, er direktørens alkoholforbrug nedskrevet i casen.

Oplysninger om dette forbrug kan misbruges, hvis der er mulighed for indsamling af oplysninger fra direktøren. Derved kan et eventuelt alkoholmisbrug påvises.

For at opsummere direktørens køb af alkohol, er nedenstående tabel en oversigt over alle punkter, hvor direktøren køber alkohol:

Punkt	Handling	Bemærkninger
4	Koncerndirektøren køber et par flasker spiritus til eget forbrug i Københavns Lufthavn, Kastrup.	Københavns Lufthavn, Kastrup registrerer køb af alkohol.
6	Koncerndirektøren benytter hotellets minibar til at forsyne sig med drikkevarer.	Ud fra hotelregningen fremgår det, hvad der er blevet taget fra minibaren på værelset.
7	Koncerndirektøren og sekretæren spiser middag på restaurant i Göteborg.	Det er her ikke oplyst, om direktøren drikker vin ell. andet til maden. Men det er muligt via regningen fra restauranten at se dette.
8	Koncerndirektøren benytter desuden hotellets room-service til at få bragt natmad og en enkelt drink op på værelset.	Ud fra hotelregningen fremgår det bestilte, der er udleveret ved roomservice.
11	Koncerndirektøren køber en dansk avis og et par drinks med sit kreditkort, mens han venter på at blive boardet i lufthavnen i Göteborg.	Via transaktionsoplysninger i forbindelse med brug af kreditkortet, fremgår det, at direktøren har benyttet kreditkortet på en bar i lufthavnen.

Om man kan kalde overstående alkoholforbrug for et misbrug er nok en vurderingssag. Men hvis disse oplysninger falder i forkerte hænder, ville de måske kunne bruges imod direktøren.

4. Scenen sættes – problematisering over privacy

For at give et overordnet billede af de realiteter, problemstillinger og dilemmaer, der knytter sig til privacy, er der nedenfor fremhævet nogle vigtige elementer, som nationalstaterne må erkende og tage stilling til på vejen imod beslutning og handling:

Erkendelsens vej til beslutning:

- Vi må erkende, at verden er forandret – og den kan ikke skrues tilbage. Den teknologiske udvikling forandrer fortsat verden.
- Vi må acceptere, at "de nordiske demokratiske rettigheder er truet" i takt med den teknologiske udvikling – men ikke dem alle. Måske er det sådan, at demokratiet netop kun overlever, fordi det bliver udfordret.
- De nordiske stater må melde ud – at verden af i dag er anderledes – **og må fortælle borgerne om det.**
- George Orwells skræmmebillede er en realitet, og er gledet over i historien – for virkeligheden er løbet fra den.
- **Vi må omdefinere privacy – definitionen er ikke tidssvarende til det teknologiske stadie og befolkningens adfærd.**
- Vil borgerne have privacy – eller er det bare noget politikerne tror?
- Vil borgerne ikke hellere have muligheder i dagligdagen? Muligheder for effektivitet, fleksibilitet mv. ved brug af teknologien øger i dagligdagens små handlinger risikoen for afkald på privatlivets fred.
- Vil borgerne ikke gerne overvåges for større sikkerhed?
- Ønsker Norden i virkeligheden fuld privacy for borgerne med risiko for rigets sikkerhed?
- Giver overvågningen faktisk øget sikkerhed og kan det forhindre de professionelle kriminelle, som kan omgå overvågningen?
- Med teknologien kan borgeren i dag være anonym, hvis mulighederne udnyttes. Hvis samfundet **vil privacy – hvorfor fremmes den privatlivsfremmende teknologi ikke i større grad?**
- De nordiske lande kan ikke styre globaliseringen eller den teknologiske udvikling. EU kan heller ikke. Verden kan (måske) – på længere sigt.
- Staten ændrer rolle, fra selv at sikre privacy-data til nu at afgive data til private virksomheder. Fører staten i praksis kontrol hermed **– og tager konsekvenser af eventuelle svigtende kontroller i virksomhederne.**
- Teknologien og dens anvendelsesmuligheder er (gøres) kompleks og i mange sammenhænge dermed uforståelig for borgerne. Borgerne må have tillid til, at fagstaben og lovgiver kan overskue konsekvenser og muligheder. **Nordisk Ministerråd skal etablere grundlag for denne tillid.**

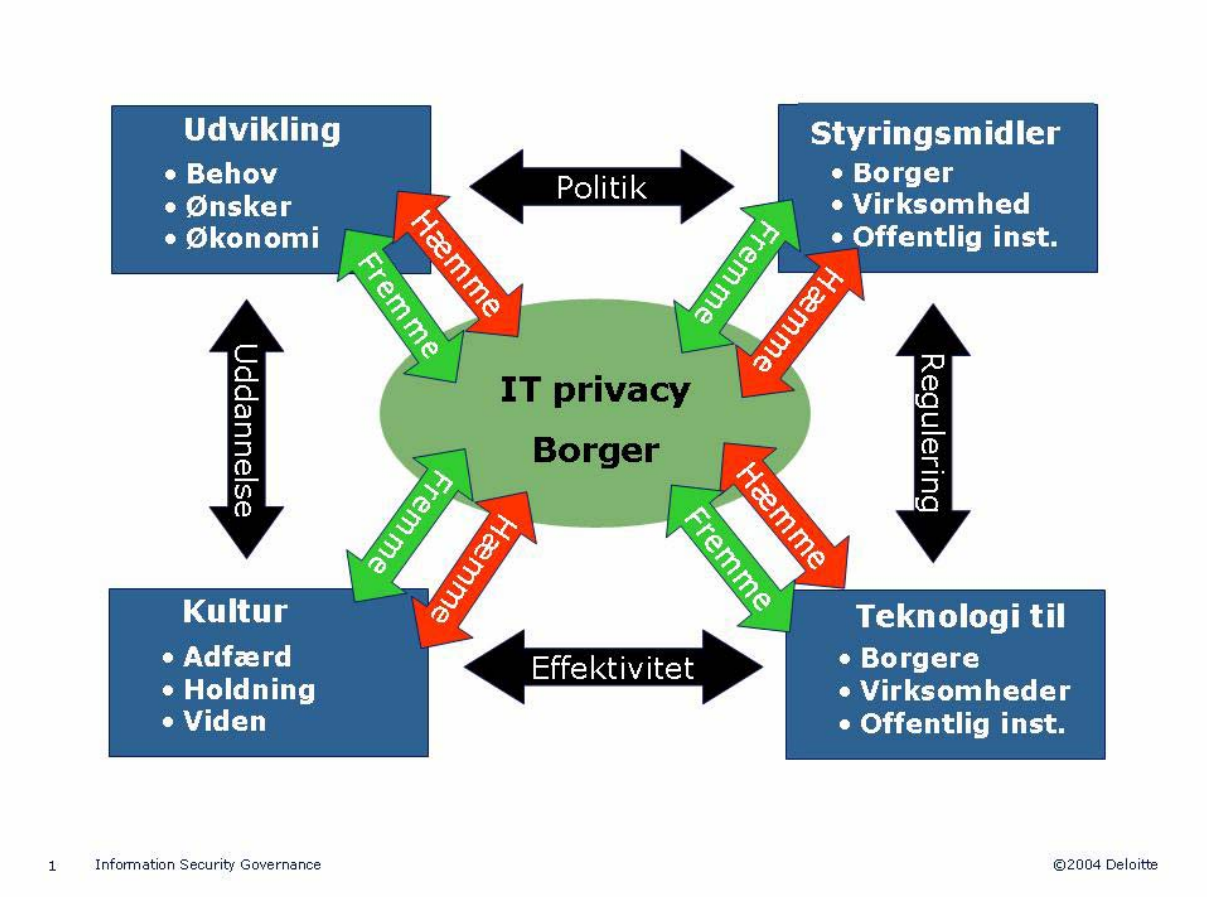
- Borgerne skal informeres og uddannes til at udnytte teknologien på en måde, så privacy stadig er en mulighed. **Nordisk Ministerråd og staterne har en stor rolle at spille her.**

5. Potentielle privacy-dilemmaer til debat

Privacy eller privatlivets fred kan forstås både snævert med udgangspunkt i de oplysninger, som lov om personoplysninger definerer det – eller mere bredt som privatlivets fred. Der findes ikke i dag en anerkendt international definition af dette begreb, og vi har derfor i denne rapport valgt at anvende den brede fortolkning. Dvs. når vi bruger privacy som begreb, så tænkes på muligheder og rettigheder for at være privat, i fred, anonym mv.

Sammenhænge og relationer mellem de forhold og elementer, der bl.a. har indvirkning på it-privacy, er illustreret nedenfor i figur 2. Denne er et forsimplet billede af en kompliceret virkelighed, og har derfor alene til formål som en forståelsesramme at illustrere de dilemmaer og udfordringer, vi foreløbig og overordnet set kan nævne.

Figur 2



Privatlivsfremmende, henholdsvis privatlivstruende forhold initieres fra og tager sit afsæt i flere forskellige faktorer, som hver især og i sammenhæng har indflydelse på det niveau af it-privacy, der måtte være i et givet samfund.

Samfundet, forenklet bestående af myndigheder (lovgivende, udøvende og dømmende), virksomheder (offentlige og private), samt borgere, er de aktører, som i interaktion skaber de ønsker og behov, der måtte være for etablering af en styringsrelation, med det mål at fastholde eller forandre niveauet af it-privacy.

Aktørerne eksisterer ikke i et vakuum, men er dels påvirket af de andre aktører, dels de samfundsmæssige, politiske, økonomiske, teknologiske og kulturelle betingelser, der måtte være på et givet tidspunkt. Herunder den stigende globalisering og samarbejdet på tværs af landegrænser. Problemstillingen må således ses i et globalt perspektiv, hvor såvel teknologier som aktører kun i meget begrænset omfang kan styres ensartet, og hvor der samarbejdes såvel mellem myndigheder/efterretningsvæsener som mellem kriminelle aktører.

Styringsrelationen kan alligevel udmøntes som lovgivning, reformer, tilskud og information med videre i nationalt eller regionalt regi. Formålet hermed kan bl.a. være at ændre borgere og virksomheders kultur, herunder vidensniveau, holdning og konkret adfærd til anvendelsen af teknologien i hverdagen. Om den konkrete adfærd matcher de samfundsmæssige ønsker og behov, vil herefter påvirke en eventuelt ændret styringsrelation.

Begrebet it-privacy og det niveau, som dette må siges at være på, vil være en sum eller et produkt af bl.a. disse beskrevne faktorer, som i et komplekst univers er afhængige af hinanden, og hvor den samlede effekt overstiger summen af de enkelte dele. En ændring af én faktor skal altid ses i sammenhæng med de andre faktorer, som i et dynamisk udviklingssystem. Ingen af forholdene vil være konstante, når der sker en påvirkning af systemet.

Vi vil i det efterfølgende debattere udvalgte potentielle privacy-dilemmaer i dette billede:

6. Teknologi

Fokus på teknologiens anvendelse over for forblændelse af teknologiens egenskaber

I vores delrapport 2 findes en liste over anvendte teknologier, samt en beskrivelse af hvilke potentielt privatlivsfremmende (PET) og privatlivstruende egenskaber (PIT) disse har. Ud fra denne liste er der meget få teknologier, der alene kan betegnes som enten rene PET eller PIT teknologier. Endvidere viser vores undersøgelse, at der i debatten om teknologier ikke findes en entydig og klar definition af, hvad der er en teknologi, og hvad der bare er en enhed eller en brugergrænseflade til teknologien.

Teknologioversigten i delrapport 2 lister udvalgte teknologier, som har været relevante i relation til privacy igennem de seneste årtier. De fleste teknologier, som er relevante i relation til privacy, er relateret til computerudviklingen, som har tilført følgende egenskaber til teknologierne af relevans for privacy:

- **Lagerplads** – Moderne harddiske og databaseteknologi yder næsten ubegrænset lagerplads for logning og opbevaring af persondata.
- **Analyse** – Med computerne er det muligt at søge på tværs af informationer globalt. Derudover er datamining blevet muligt på et helt nyt plan.
- **Størrelse** – Den nyeste udvikling af microchips har gjort computerne så små og billige, at mennesker i dagligdagen er tilkoblet langt flere PET og PIT teknologier.
- **Pris** – Computerkraft og lagerplads er blevet tilgængelig for en langt større brugergruppe, selv private brugere har i dag i vid udstrækning ressourcer til at opbygge omfattende databaser og lave komplekse analyser.

Det, som mange opfatter som teknologier, er mere en brugergrænseflade til de egentlige teknologier. Således er e-mail ikke en teknologi, men en brugergrænseflade, der gør det muligt at udnytte teknologien, som f.eks. Internettet er bygget op omkring: Netværksprotokoller, der transporterer kommunikation via telefonkabler. Sikring af privacy ved kommunikation via e-mail kan ske ved anvendelse af den privatlivsfremmende teknologi, som betegnes kryptering. Et andet eksempel er mobiltelefonen, som ikke er en teknologi, men en enhed, der bruger mobilteknologien til at kommunikere via forskellige netværksprotokoller – GSM[5], GPRS[6] og MMS[7], der transporteres via radiobølger.

[5] (Global System for Mobile Communication). En europæisk digital standard for mobiltelefoner.

[6] (General Packet Radio System). En trådløs datatransmissions service/protocol.

[7] (Multimedia Message Service). En metode til at transmittere grafik, videoklip, lydklip og tekst over trådløst netværk ved brug af WAP-protokollen.

Både radiobølger og telefonkabler er gammel teknologi, som anvendes i forbindelse med andre teknologier for at tilbyde brugerne en let tilgængelig og forståelig brugergrænseflade. Dermed opstår der forvirring i debatten om, hvorvidt en teknologi som e-mail er potentielt fremmende eller hæmmende for privacy.

Teknologiernes kombination, relationer og anvendelse er afgørende for, om de er potentielt fremmende eller hæmmende for privacy. Således vil e-mail uden kryptering være privatlivshæmmende, fordi man på Internettet og mail-serverne (posthuse) ikke har de samme kontroller, som man gennem årtier har indarbejdet omkring traditionel brevforsendelse via postvæsenet. Kontroller, som er manuelle, med det formål at sikre brevhemmeligheden. Den samme beskyttelse ligger ikke i de digitale posthuse. Lovgivningen omkring sikring af brevhemmelighed gælder dog stadigvæk for e-mail, men det er ikke muligt for forbrugeren at se (opdage), når nogen bryder denne lov. Dertil kommer, at de eksisterende kontrolforanstaltninger fra datatilsynet og sanktionsmuligheder i form af domstolsafgørelser ikke er imponerende, og derfor ikke virker præventivt.

I relation til bevarelse af privacy, når der kommunikeres via e-mail og telefoni, ville borgerne være meget bedre stillet, hvis de anvender kryptering. Men dette er ikke altid muligt, da denne facilitet ikke stilles til rådighed i alle e-mail-programmer eller ved telefoni. Borgeren skal selv aktivt gøre noget f.eks. ved at anvende digital signatur eller telefoniprogrammer som Skype, der kommunikerer krypteret over Internettet.

Kryptering sikrer dog kun mod, at andre kan få kendskab til indholdet af kommunikationen. Borgeren er ikke beskyttet mod, at der foretages registrering/logning. Ved telefoni registreres, hvem der taler med hvem, idet telefonnummer og simkort-nummer registreres. Og ved brug af e-mail registreres afsenderadresse, og netværkskortets mac-adresse.

Vi kan alle som borgere optræde anonymt i vores kommunikation, men det kræver en del teknisk viden og kunne, og er derfor ikke en mulighed for alle. Vi må antage at professionelle kriminelle ved hvordan man kommunikerer anonymt – og udnytter disse muligheder. Dermed er det kun alle lovlydige borgere, som reelt set udsættes for privacy-krænkende registreringer, mens de personer, som myndighederne ønsker at identificere, overvåge og tilfangetage kan gå fri, som oftest grundet særlige it-kundskaber.

I vores delrapport 3, har vi vurderet de anvendte teknologier i forhold til, om de umiddelbart overholder lovgivningens forskellige krav i relation til privacy. En af hovedkonklusionerne er, at mange af de anvendte teknologier, som vi kender i dag forudsætter, at en systemadministrator eller anden professionel bruger udfører en tilpasning af opsætningen af teknologien for at sikre privacy ved anvendelsen heraf.

Den kompleksitet og særlige viden, som de teknologiske muligheder har introduceret i forbindelse med sikring af privacy gør, at man som borger ikke alene skal have tillid til, at staten sikrer ens privacy-rettigheder, men nu også skal have tillid til, at alle de systemadministratorer, som er ansvarlige for at konfigurere teknologier rundt omkring i virksomheder og offentlige institutioner, varetager denne opgave for at sikre privacy for borgerne.

Sammenfatning

Politiske udfordringer	**Løsninger**
Der mangler en klar definition af teknologi i relation til privacy.	• Fastlæggelse af definitionen af teknologi på nordisk plan.
Borgerne er ikke i stand til at anvende de forskellige teknologier til sikring af privacy.	• Information til borgerne om, hvorledes de anvender forskellige teknologier til sikring af privacy.
De muligheder, der findes i teknologierne, er ikke altid stillet til rådighed fra leverandøren, f.eks. kryptering af telefonsamtaler.	• Staten skal tvinge leverandørerne til at stille privatlivsfremmende tiltag til rådighed, eller selv udbyde services, som gør, at borgerne kan være anonyme.
Kontrol og overvågningstiltag, der iværksættes for at opdage, overvåge og fange kriminelle har ikke altid den ønskede effekt. De professionelle kriminelle kan anvende privatlivsfremmende teknologier til at gøre sig anonyme. Kontrol og overvågning rammer i stedet den lovlydige borger.	• Staten bør informere borgeren, så de har samme muligheder for at være anonyme som de kriminelle. • Der bør ikke indføres privacy-krænkende tiltag, som kun svagt rammer målgruppen (kriminelle), men som fuldt ud rammer de almindelige borgere.
Sikring af privacy varetages ikke længere alene af staten, men er lagt ud til systemadministratorer i private virksomheder (nordiske eller internationale virksomheder).	• Staten bør varetage kontrollen over væsentlige privacy sikrende tiltag. • Staten bør føre effektivt og konsekvent tilsyn med virksomheder, som driver teknologier, der har privatlivshæmmende effekt på privacy.

Anvendelsen af teknologi giver brugeren fordele

Vi befinder os i starten af den teknologiske tidsalder, hvor teknologien for borger, virksomheder og myndighed er midlet til forbedring af mange af vores dagligdagssituationer. For eksempel kan lettere kommunikation og informationsadgang på alle geografiske steder og tider af døgnet opleves af borgeren som forbedret livskvalitet og service, mens det for virksomheder og myndighed giver en effektivisering og økonomisk gevinst.

Derved er der tilsyneladende skabt en positiv gevinst for alle parter. Men da muligheden for kommunikation og informationsadgang stiller nogle krav til brugerne – ofte borgerne – som medfører afgivelse af information, der lagres elektronisk, kan denne information være potentielt privatlivstruende. Endvidere forudsætter det ofte, at borgerne selv etablerer nødvendige sikringsforanstaltninger til fremmelse af privacy ved anvendelse af teknologien. Ofte er de private informationer ikke nødvendige for brug af teknologierne, men de har en kommerciel værdi for forhandleren/leverandøren.

Der er teknologier, som Radio Frekvens ID (RFID)[8], der i dag i stigende omfang tages i anvendelse på mange forskellige områder, f.eks. i fødevarer, tekstiler og elektronik. På grund af størrelsen af RFID-chippen er det kun fantasien og behovet, der sætter grænsen for anvendelsen. Anvendelsen er i dag – så vidt vi ved - på en sådan måde, at den ikke behandler information, der har privacy-relevans ud fra definitionen af privacy i dag. Anvendelsen af RFID burde derfor ikke give anledning til privacy-bekymring. Men den mulige sammenstilling af informationer fra RFID (hvilket er en anvendelsesform) i form af privacy-informationer (forbrugsmønstre) kan medføre, at det er muligt at tegne et meget detaljeret billede af et enkelt individs færden og gøren. Et tydeligt eksempel på dette er RFID-chip i brugsgenstande som tøj, elektroniske apparaturer, køretøjer m.m. Informationen i sig selv fortæller ikke noget om personen, der anvender tøjet, apparatet, køretøjet. Men i det øjeblik, man kan kæde denne information sammen med en person, bliver informationen potentielt krænkende for privatlivet.

Teknologierne og deres kendetegn, som de er beskrevet i delrapport 2, kan bruges som inspirationskilde til løbende at vurdere, om de styringsmidler, som i dag anvendes til at sikre privacy, er tilstrækkelige ved den nuværende og fremtidige anvendelse af ny teknologier.

Sammenfatning

Politiske udfordringer	**Løsninger**
Mange leverandører afkræver borgerne privacy-information, før man kan anvende den ønskede teknologi. Ofte information, som er irrelevant i forhold til anvendelsen, men som kan udnyttes kommercielt af leverandøren.	• Staten kan informere borgerne om konsekvenser ved afgivelse af personlig information. • Staten kan lovgivningsmæssigt begrænse mulighederne for indsamling af information. • Staten skal skabe muligheder for, at brugere kan være anonyme ved. f.eks. færden på nettet.
Nye teknologier, der registrerer information, som grundlæggende ikke er privacy-krænkede, f.eks. RFID-registreringer, kan få en voldsom effekt på privacy i det øjeblik, de kædes sammen med personoplysninger.	• Staten bør være særlig opmærksom på mulighederne i nye teknologier og forsøge at påvirke udviklingen ved at stille krav og definere standarder, så privacy sikres. • Staten bør sikre mod, at data sammenkædes, således at registreringen af borgernes gøren og laden ikke misbruges. • Staten bør sikre, at den eksisterende lovgivning på området udfyldes med klare krav og mål. Staten bør etablere tiltag så det sikres, at denne lovgivning overholdes.

[8] RFID afgiver kontinuerligt et signal om sin position med få informationer, som ofte er et identifikationsnummer, som kan aflæses trådløst af en RFID scanner. Denne aflæsning kan foretages over afstand.

Effektiv anvendelse af teknologien på bekostning af statslig kontrol

Hvad enten det skyldes politisk uvilje, manglende forståelse af problemet eller økonomisk prioritering, så udnyttes de privatlivsfremmende teknologier ikke effektivt nok til sikring af borgernes privacy.

Der vil altid være behov for at foretage en afvejning mellem beskyttelse af borgernes privacy-interesser over for statens interesser, som f.eks. i forhold til bekæmpelsen af terror.

Der er dog områder, hvor der findes teknologiske løsninger, som kan hjælpe den enkelte borger med beskyttelse mod en væsentlig del af de privacy-trusler, der går under betegnelsen spam, og som ikke strider mod statens interesse. Spam skal i denne forbindelse opfattes bredt og kan kategoriseres i følgende tre typer:

1) Kommercielle såvel som ikke kommercielle beskeder, der massefremsendes uopfordret til brugeren, typisk via e-mail eller sms.
2) E-mail-beskeder og programmer, der forsøger at lokke brugeren til at afsløre personlige oplysninger om brugeren f.eks. via Phishing.
3) Aktive programmer, der kan forrette skade, som følge af f.eks. destruktion af data, virus, spyware, backdoors mv.

En af problemstillingerne ved anvendelsen af mere effektive tiltag til bekæmpelse af spam er, at udgifterne til etablering og drift af tiltagene ikke er fastlagt. Hvem skal betale?

Da det er borgerne som rammes, kan man have den holdning, at de også skal bære omkostningen. De har måske bare ikke den fornødne forudsætning for at sikre sig imod spam. Spam rammer også virksomheder og de offentlige institutioner, og de burde måske bære udgiften, da de har en kommerciel interesse i at kunne anvende deres systemer effektivt. Et tredje synspunkt kunne gå på, at udbyderne af internetydelser (ISP'erne) skal stille effektive tiltag til rådighed og bære en væsentlig del af omkostningerne.

Uanset hvad det enkelte land gør, vil en effektiv løsning kræve en global løsning, og her ligger det reelle problem. Selv inden for de nordiske lande er der, ifølge vores analyse i delrapport 4, ikke enighed om løsninger, og der er etableret forskellige tiltag uden en effektiv koordination. Men et ensartet nordisk tiltag er ikke tilstrækkeligt. Et effektivt tiltag kræver en global løsning.

Man har internationalt talt om dette problem siden 1999, men der er stadig ikke sket noget. Senest er en række ISP'ere dog blevet enige om samlet at bekæmpe spam. Hvis problemet er vigtigt nok for politikkerne, så burde der allerede være igangsat tiltag, som kan afhjælpe problemer evt. i samarbejde med ISP'erne.

En regulering mod spammere skal have tilknyttet nogle konsekvente og effektfulde sanktioner. Der er ikke meget konsekvens bag de styringsmidler, de nordiske lande har etableret, idet der er meget få domsfældelser for de overtrædelser, som er anmeldt. Man kan også vurdere, om bøderne har en tilstrækkelig størrelse, så det har en præventiv virkning, når gevinsterne for krænkeren af privacy kan være meget være større end bøderne.

Sammenfatning

Politiske udfordringer	**Løsninger**
Løsninger til bekæmpelsen af spam kræver økonomiske midler – finansiering.	• Staten bør allokere økonomiske ressourcer til etablering af effektiv bekæmpelse af spam. • Staten kan lovgive om, at ISP'erne skal bekæmpe spam. • Staten kan skabe muligheder for borgerne, så de selv kan bekæmpe spam.
Effektive løsninger mod spam skal være globale.	• De nordiske lande bør fortsætte deres arbejde i de internationale fora. • De nordiske lande bør skabe fælles nordiske løsninger.
Der er i praksis effektueret meget få sanktioner i form af bøder og domme mod spammere.	• Staten bør være mere konsekvent og forfølge lovovertrædere.

7. Kultur

Demokratiske rettigheder eller teknologiske gevinster

De nordiske velfærdsstater har en lang demokratisk historie, hvor vi bryster os af at have en høj standard for beskyttelse af det enkelte individs personlige frihed og rettigheder. Historisk har vi i Norden beskrevet de demokratiske rettigheder ud fra efterlevelsen af vores forfatningsmæssige lovgivninger/ Grundloven. I disse er den personlige frihed fremhævet som en ukrænkelig ret for alle borgere uanset politisk, religiøs eller racemæssig baggrund.

Ligeledes har de nordiske lande og mange flere lande tilsluttet sig FN's verdenserklæring om menneskerettighederne, ligesom den europæiske menneskerettighedskonvention er implementeret ved national lovgivning. I artiklerne heri gives enhver borger bl.a.:

- Ret til liv, frihed og personlig sikkerhed
- Ret til at være lige for loven
- Ret til at bevæge sig frit og forlade et hvilket som helst land
- Ret til tanke-, samvittigheds- og religionsfrihed
- Ret til menings- og ytringsfrihed

Disse rettigheder prøver langt de fleste stater at efterleve. Den teknologiske udvikling, som vi har beskrevet den i delrapport 2, muliggør dog, at staterne kan etablere overvågning og kontrol af borgerne og deres adfærd. Samtidig giver nogle af teknologierne mulighed for, at borgerne kan undgå overvågning f.eks. i relation til deres adfærd på Internettet eller brug af mobiltelefoner.

Er en overvågning af individets bevægelser, adfærd og handlinger en trussel mod de demokratiske rettigheder, som vi i Norden kalder vores, og som vi til alle tider er parate til at forsvare, når vi bliver adspurgt? Truslen mod disse rettigheder er stærkt stigende, da flere mindre tilbageskridt sammenlagt udgør en større trussel, end vi i nyere tid har været opmærksom på. Hver for sig synes det ikke som store krænkelser, at der etableres videoovervågning i busser og tog, eller at telefonsamtaler registreres. Men muligheden for at kombinere data fra flere registre og databaser omkring den enkelte person udgør en stigende risiko for potentiel krænkelse af privatlivets fred.

Er privacy-debatten en global debat og et globalt menneskeretligt problem, eller er det på grund af vores historie, kultur og velfærdsstatslige reguleringsformer et nordisk fænomen? Vi definerer privacy ud fra de nordiske normer omkring demokrati. Normer som måske ikke længere er tidssvarende i forhold til den økonomiske udvikling og den globale verdensorden, der hersker.

Sammenfatning

Politiske udfordringer	**Løsninger**
Den teknologiske udvikling muliggør, at staterne kan etablere overvågning og kontrol af borgerne og deres adfærd.	• Borgerne må sikres, så overvågningsdata og kontrol med adfærd udelukkende anvendes af myndighederne til det rette formål. • Staten må sikre, at overvågningsdata opbevares og anvendes betryggende. • Staten må give borgerne information om, hvordan man kan undgå overvågning, f.eks. i relation til deres adfærd på Internettet eller brug af mobiltelefoner.
Truslen mod de nordiske demokratiske rettigheder er stærkt stigende pga. flere mindre tilbageskridt, der sammenlagt udgør en større trussel, end vi i nyere tid har været opmærksomme på.	• Staten må sikre, at overvågningsdata og kontrol med adfærd udelukkende anvendes af myndighederne til det rette formål.
Vi definerer privacy ud fra de nordiske normer omkring demokrati. Normer som måske ikke længere er tidssvarende i forhold til den økonomiske udvikling og den globale verdensorden, der hersker.	• De nordiske lande må igangsætte en debat omkring privacy-begrebet, også blandt borgerne. • De nordiske lande må tage initiativ til en international debat omkring privacy. • De eksisterende tiltag til sikring af privacy skal ajourføres i forhold til den opdaterede privacy-definition. • Der skal identificeres supplerende og nye tiltag til sikring af privacy på områder, hvor bl.a. lovgivningen ikke giver tilstrækkelig sikring.

Kommunikation om privacy til alle eller kun til de få?

At forstå udviklingen og problemstillingerne i informations- og kommunikationsteknologien kræver i høj grad specialiseret viden. Viden, som ikke er let at kommunikere videre til den enkelte bruger og borger på et niveau, der gør den forståelig og anvendelig for alle. Hvis ingen tager ansvar for kommunikationen, og hvis denne ikke målrettes brugeren/borgeren, kan man ikke forvente, at denne ændrer adfærd i anvendelsen af teknologien. Ønsker lovgiver og myndigheder derimod, at borgeren skal ansvarliggøres og initiere til ændret adfærd, må dette kombineres med en intensiv og fokuseret information.

Omvendt vil en meget detaljeret kommunikation og information omkring risici ved anvendelsen af de forskellige teknologier kunne skræmme borgerne med den konsekvens, at de ikke tør udnytte denne. Et eksempel herpå er handel via Internettet, som mange borgere ikke anvender på grund af usikkerheden i forbindelse med betaling over nettet.

Sammenfatning

Politiske udfordringer	**Løsninger**
Problemstillingerne i informations- og kommunikationsteknologien kræver i høj grad specialiseret viden. Viden, som ikke er let at kommunikere videre.	• De offentlige myndigheder skal tage ansvar for en informations- og kommunikationsstrategi til borgerne omkring risici for privatlivets fred ved anvendelsen af de nye teknologier.
Detaljeret information omkring risici ved anvendelsen af de forskellige teknologier kan skræmme borgerne, så de ikke udnytter teknologien.	• De offentlige myndigheder skal fremstå som en troværdig formidler af information omkring risici ved anvendelsen af teknologierne.

Teknologiens potentiale for demokratisk deltagelse

Teknologien giver mulighed for etablering og deltagelse i en elektronisk debat, hvor alle kan blive hørt uanset race, religion eller overbevisning i øvrigt. Men der er risiko for, at denne debat ikke forbliver anonym, når det med overvågning og registrering er muligt at finde frem til, hvem der har sagt hvad hvornår.

Dette vil kunne skræmme borgerne fra at deltage i den offentlige og demokratiske debat, når det synliggøres, at denne debat ikke er anonym.

Sammenfatning

Politiske udfordringer	**Løsninger**
Teknologien giver mulighed for etablering og deltagelse i en elektronisk debat, hvor alle kan blive hørt uanset race, religion eller overbevisning i øvrigt. Men der er risiko for, at denne debat ikke forbliver anonym.	• De offentlige myndigheder må sikre, at borgerne kan deltage anonymt i den elektroniske debat.

Afgivelse af national suverænitet til fordel for global regulering/samarbejde

I takt med udviklingen af informationssamfundet og den stigende globalisering er beskyttelsen af det enkelte individs frihed og anonymitet ikke længere alene et ærinde for staten. Flere og flere informationer udveksles om individerne mellem flere og flere aktører.

Styreformen var tidligere (før den store udbredelse af it) mere direkte og enkel med konkret og specifik lovgivning målrettet mod konkrete problemer omkring data, datas opbevaring og arkivering samt anvendelse. Nutidens lovgivning er i højere grad mere ramme-, norm- og adfærdsregulerende i forhold til informations- og kommunikationsteknologi. F.eks. anvendelsen af Internet. Antallet af informationer, kombinationsmulighederne imellem dem samt antallet af aktører i informationsstrømmen - såvel nationale som globale - vanskeliggør statens mulighed for entydigt at kunne regulere dataanvendelsen og beskyttelsen af det enkelte individ.

Sammenfatning

Politiske udfordringer	**Løsninger**
I takt med udviklingen af informationssamfundet og den stigende globalisering er beskyttelsen af det enkelte individs frihed og anonymitet ikke længere alene et ærinde for staten.	• De offentlige myndigheder må sikre borgernes privatlivs fred, også selv om der er flere aktører involveret nu.
Hvor styreformen tidligere var mere direkte og enkel med konkret og specifik lovgivning målrettet mod konkrete problemer omkring data, er nutidens lovgivning mere ramme-, norm- og adfærdsregulerende i forhold til informations- og kommunikationsteknologi.	• De offentlige myndigheder må på tværs af landegrænser sikre, at lovgivningsmæssige tiltag til sikring af privatlivets fred suppleres med andre tiltag, der kan medvirke til opnåelse af privatlivets fred i størst muligt omfang.

8. Udvikling

Statslig eller privat kontrol?

Staten har i Danmark i mange år lagt driften af en række væsentlige og samfundskritiske it-systemer f.eks. personnummerregistret, politiets og efterretningstjenestens it-systemer i det statskontrollerede Datacentralen. Datacentralen er siden hen solgt til den amerikanske koncern CSC, som verden over varetager drift af systemer for såvel private som offentlige myndigheder.

Senest er der tale om, at kommunernes datacenter, KMD, skal sælges, efter det er omdannet til aktieselskab. Hvem der køber et selskab som KMD, kan der kun gættes på, men det er sikkert, at det ikke bliver staten. Denne tendens ses på flere og flere områder, hvor offentlige myndigheder outsourcer deres it-systemer til private virksomheder for at opnå en økonomisk besparelse.

Såvel KMD som CSC varetager opbevaring og sikring af de mest personfølsomme oplysninger, som findes om det enkelte individ. Man kan få den opfattelse, at sikringen af borgernes privacy tilsidesættes for driftsøkonomiske årsager – en årsag der ud fra en nationaløkonomisk og et privacy-synspunkt kan være tvivlsomt, men som isoleret set måske kan give en kortsigtet besparelse i et enkelt ministerium eller kommune.

Det eneste reelle styringsmiddel, som i dag er etableret til sikring af borgernes privacy i de situationer, hvor det offentlige outsourcer deres ansvar om sikring af privacy til private virksomheder, er personoplysningsloven. Den kontrol, der ligger direkte som følge af personoplysningsloven eller indirekte i andre love eller bekendtgørelser, er efter vores vurdering i praksis ikke effektiv, da loven ikke i tilstrækkelig grad forebygger brud på privacy.

Der savnes kontrol med virksomheder, som opbevarer og behandler privacy-data samt klart definerede konsekvenser og restriktive handlinger, der kan tages i anvendelse, hvis der sker brud på loven. I praksis er det vanskeligt at opdage, om privacy-data kopieres og misbruges uden for landets grænser, men det bør ikke afholde staten i at forsøge at forebygge dette ved løbende kontrol.

Der eksisterer datatilsyn i de nordiske lande, men det synes ikke som om, at der er tilstrækkelige administrative ressourcer til at sikre den forebyggende kontrol.

Er borgernes privacy til købs? Det kunne ovennævnte indikere, men disse store ressourcestærke og kompetencetunge outsourcingvirksomheder kan i praksis sikre privacy bedre - eller mindst lige så godt som offentlige institutioner.

Kulturelt er der tale om en væsentlig ændring, idet borgerne i de nordiske lande historisk har haft større tiltro til staten end til private virksomheder.

Sammenfatning

Politiske udfordringer	Løsninger
Staten outsourcer deres drift af systemer med privacy-data – og dermed sikringen af disse data til private virksomheder.	• Man bør politisk vurdere, om det er i nationens interesse, at alle opgaver i relation til privacy-data outsources til private virksomheder. F.eks. kan det undre, at personnummerregistret og politiets oplysninger varetages af private virksomheder.
Private virksomheder, der varetager opgaver for staten, kan blive solgt til udenlandske virksomheder med anden lov og kultur, og som måske ikke har den tilstrækkelige forståelse for de nationale love.	• Staten kan sikre, at varetagelsen af opgaver i relation til privacy-data for staten, kun kan varetages af de nationale virksomheder.
Styringsmidlet i form af personoplysningsloven er ikke effektiv nok i sikringen af borgernes privacy-rettigheder over for private virksomheder.	• Staten bør stille klare krav til sikkerheden hos de private virksomheder, således at privacy for borgerne sikres. • Staten bør foretage aktiv kontrol af virksomhedernes efterlevelse af loven. • Staten bør indføre og sikre effektfulde konsekvenser ved brud på privacy.

Magten er flyttet fra staten til computernørderne

Regulering omkring privacy og styring af data indbygges nu i høj grad i udformningen af teknologierne og deres anvendelsesmuligheder frem for i konkrete love, der er målrettet den enkelte teknologi. Da lovene er teknologineutrale vil opfyldelse af lovgivningens krav til beskyttelse af data ligge i den konkrete udmøntning og anvendelse af teknologierne. Dette er en af de væsentlige konklusioner i vores delrapport 3 vedrørende vurdering af teknologiernes muligheder for at overholde lovgivningens krav.

Dette betyder, at ansvar for beskyttelse af oplysninger omkring borgernes adfærd på f.eks. Internettet nu ligger i hænderne hos de personer og virksomheder, der udvikler teknologierne og eventuelt har overordnet kontrol med disse teknologier. Når staten ikke længere kan kontrollere disse teknologier og specifikt anvendelsen af data, må tilliden nu rettes mod de specialister, der står bag teknologierne.

Et aktuelt eksempel herpå er opbevaring af og adgang til lægejournaler, som i tidligere tider alene lå hos den praktiserende læge og på hospitalet. Disse journaler har man nu i Danmark gjort tilgængelige på Internettet. Dels som elektroniske journaler, som alle relevante læger har adgang til, dels som et dokument, patienten selv ret enkelt kan få adgang til. Adgang til noget så følsomt som borgernes lægejournal via Internettet øger risikoen for, at andre uden relevant ærinde kan skaffe sig adgang hertil. Staten bør i et sådan tilfælde føre særligt tilsyn med sikringen af brud mod privacy.

Sammenfatning

Politiske udfordringer	Løsninger
Når staten ikke entydigt kan kontrollere disse teknologier og specifikt anvendelsen af data, må tilliden nu rettes mod de specialister, der står bag teknologierne.	• Staten bør stille klare krav til sikkerheden hos de private virksomheder, således at privacy for borgerne sikres. • Staten bør stille krav omkring indarbejdning af privacy foranstaltninger i udviklingen af teknologier. • Staten bør foretage aktiv kontrol af virksomhedernes efterlevelse af loven. • Staten bør indføre og sikre effektfulde konsekvenser ved brud på privacy.

Global udvikling med overvågning og kontrol

Internationaliseringen, globaliseringen og den grænseoverskridende handel øger behovet for at udveksle informationer over grænserne. Ligeledes kan kriminaliteten i form af terror bevæge sig fra at være et nationalt problem til at være et international mål - og dermed problem. Terroren har siden flykapringen opstod været synligt internationalt. I de seneste år har terroren taget en dramatisk drejning i retning af et globalt terrornetværk, som ikke ønsker forhandling, men omvæltning og forandring.

Det internationale samfunds reaktion herpå er en øget kontrol og overvågning af offentlige steder og dermed en registrering af borgernes færden og aktivitet på disse steder. Dette suppleret med logning/registrering af al kommunikation, herunder e-mail og talekommunikation mellem borgere i de enkelte land og på tværs af landegrænserne.

Staterne er parate til at udveksle denne information, såfremt det fremmer opklaring af terror eller kriminel handling. Et effektivt værktøj i opklaring og pågribelsen af de indblandede i 11. september terroren og London-bombningen. Men de egentlige bagmænd har man ikke kunne pågribe endnu.

Den øgede overvågning og kontrol går klart imod ønsket om bevarelsen af borgernes privacy. En omkostning, som mange nok er villig til at betale, hvis man har en sikkerhed for, at oplysningerne ikke blev misbrugt og en tro på, at overvågningen reelt set giver et højere sikkerhedsniveau.

For de borgere, som har en stor og tilstrækkelig viden om teknologiernes mulige privacy-fremmende egenskaber, er bevarelsen af privacy kun gjort vanskelig – men ikke umulig – i relation til den øgede overvågning og kontrol. Det er således muligt med computerteknologien at undgå personhenførbar registrering af e-mail, web-browsing, Internet debatfora og tale-kommunikation via Internettet, ved brug af kryptering og teknologier til sløring af de elektroniske spor.

Denne mulighed har de kriminelle selvfølgelig også. Ligesom de sandsynligvis også har flere muligheder, da de sandsynligvis ikke har problemer med at bryde det regelsæt, der begrænser den normale

lovlydige borgers. F.eks. ved at udgive sig for at være en anden, når de har hacket sig ind på andre borgeres computere og misbruger deres udstyr og adresser m.m., eller ved at anvende stjålent udstyr. Hertil kommer, at de kan udføre deres kriminelle handlinger fra et andet land, som måske ikke har helt så stramme regler for disse aktiviteter.

Sammenfatning

Politiske udfordringer	**Løsninger**
Tiltag, som begrænser borgernes privacy-rettigheder for at fange kriminelle, er ikke entydigt effektive.	• Staten skal sikre, at et tiltag, der umiddelbart virker effektivt i kampen mod kriminaliteten, men som krænker borgernes privacy-rettigheder, ikke kan omgås af de kriminelle, og dermed alene har en negativ effekt på privacy. Det kan man påstå er tilfældet med logning af tale- og e-mail kommunikation. Det kan dog have sin berettigelse, idet kommunikation er vanskeliggjort for de kriminelle. Men er prisen for høj i relation til borgernes privacy-rettigheder?
Tiltag til sikring af privacy skal koordineres internationalt for at sikre mod internationalt misbrug.	• Verdens stater bør indgå samarbejde om fælles lovgivning, tiltag og kontrolforanstaltninger til sikring af borgernes privacy-rettigheder internationalt.

9. Styringsmidler

Hvordan styrer man privacy-reguleringen, når privacy ikke er klart defineret?

Den første definition af privacy blev givet af en amerikansk højesteretsdommer tilbage i 1890'erne. Den dag i dag findes der ikke én entydigt anerkendt definition af privacy. I den digitale verden taler man ofte om privacy som beskyttelse af person-oplysninger, men også som et bredere begreb relateret til den personlige integritet og selvbestemmelse.

Grundlæggende kan man sige, at det drejer sig om borgernes ret til i fred uden indblanding og overvågning af andre at bestemme, hvad man vil offentliggøre om sig selv og under hvilke omstændigheder, såfremt man ellers overholder gældende lov. Set i lyset af den stigende kriminalitet og terrorvirksomhed bør man vurdere, om dette overhovedet er muligt og acceptabelt for samfundet i dag.

Den teknologiske udvikling har inden for de sidste år tydeliggjort behovet for fastlæggelse af begrebet privacy og i den forbindelse reformulere og redefinere de lovtiltag, der dækker dele af privacy-området. Vores analyse i forbindelse med delrapport 1 viser, at de nordiske tiltag til sikring af privacy, styret ved personoplysningsloven, ikke i tilstrækkelig grad afspejler det teknologiske stadie og de ønsker, der måtte være til sikring af privacy-rettighederne i fremtiden.

Der kan ikke sættes lighedstegn mellem definitionen af personfølsomme data og privacy-data, hvis privacy data skal omfatte alle oplysninger, som kan genkende borgeren som individ. Således dækker personfølsomme oplysninger i persondataloven f.eks. ikke i alle tilfælde fingeraftryk og DNA. I de tilfælde, hvor disse biometriske data lagres på en sådan måde, at den registrerede ikke kan identificeres, betragtes data ikke som personoplysninger.

Ønskerne til indholdet i privacy-definitionen vil være forskellig afhængig af, om det er borgeren, en privat virksomhed eller de nationale stater, der formulerer definitionen, da der er forskellige interesser. Ligeledes kan man forestille sig, at der vil være regionale forskelle, således at Norden på baggrund af vores demokratiske traditioner eventuelt har en anden forståelse for omfanget af privacy. Netop på baggrund af disse traditioner kan det i Norden være hensigtsmæssigt at rejse sagen til offentlig debat, således at borgeren har muligheden for at komme med indlæg. Privacy bør tage udgangspunkt i borgernes rettighed – demokratiet er borgernes rettighed.

Den manglende entydige definition af privacy gør debatten i medierne uklar. Ligesom den for myndighederne afstedkommer dels etablering af utilstrækkelig styringstiltag til sikring af borgernes rettigheder, dels (måske ubevidst – grundet ugennemsigtighed) krænkelse af privacy-rettighederne som følge af kontrol og overvågningstiltag, der tilgodeser statens interesse.

I debatten er det ligeledes nødvendigt at forklare privacy i relation til teknologierne og deres mulige anvendelser, og dermed risiciene for tab af privacy. Det er en stor informationsmæssig udfordring på den ene side at give tilstrækkelig og detaljeret information, uden at dette samtidig skræmmer borgerne, så den nye teknologi ikke bliver brugt.

Vores analyse i delrapport 3 viser, at problemstillingerne er meget tekniske og på nogle områder kræver specialiseret viden. Mange teknologier kan konfigureres, så lovene omkring beskyttelse af personlige oplysninger bliver overholdt, men det kræver ofte specielle kompetencer enten fra en professionel bruger eller ved, at det indbygges i teknologien. Det vil være nødvendigt med information herom på en forståelig og brugbar form til den almindelige bruger af teknologierne, hvis borgerne selv skal kunne opretholde privacy ved anvendelsen af teknologierne.

Sammenfatning

Politiske udfordringer	**Løsninger**
Privacy er ikke entydig defineret, hvilket vanskeliggør en meningsfuld debat samt besværliggør myndighedernes fastlæggelse af hensigtsmæssige og effektive styringsmidler.	• Man bør på globalt plan eller alternativt nordisk plan fastlægge definitionen af privacy. • De statslige myndigheder bør initiere en offentlig debat omkring privacy.
Eksisterende styringsmidler i form af persondataloven dækker ikke nye typer informationsregistreringer som f.eks. billeder, bevægelsesdata og fingeraftryk som følge af nye teknologier.	• Eksisterende styringsmidler i form af lovgivning skal reformuleres og redefineres til den brede opfattelse af privacy, så loven også dækker anvendelsen af nye teknologier.
Det er en stor informationsmæssig udfordring på den ene side at give tilstrækkelig og detaljeret information, uden at dette samtidig skræmmer borgerne, så den nye teknologi ikke bliver brugt.	• Udvikling/tilpasning af informationsstrategi. • Iværksættelse af målgruppefokuserede informationskampagner.

Fra national lovgivning til globale tiltag

Udviklingen i samfundet betyder, at vi i den internationale verden oplever, at grænser mellem kontinenter, lande, it-systemer og individer brydes ned. Lovgivningen omkring beskyttelse af personoplysninger tager i Norden udgangspunkt i den nationale lovgivning, som for nogle er en implementering af EU-lovgivningen.

Trods ønsket om harmonisering viser delrapport 1, at der er forskelle imellem de nordiske landes databeskyttelseslovgivning. Forskellene findes i den registreredes indsigelsesret, kategoriseringen af oplysningerne og ikke mindst med hensyn til de love, der udstedes for fravigelse af personoplysningsloven i de enkelte lande.

Dette gør det svært at sikre den enkelte borgers privacy-rettigheder i en stigende international verden, hvor data bevæger sig på tværs af landegrænserne. Dermed er privacy-beskyttelsen reelt aldrig bedre end den, der gives i det land med den ringeste beskyttelse. Kæden er ikke stærkere end det svageste led, hvis fuldstændig harmonisering ikke vælges.

Sammenfatning

Politiske udfordringer	Løsninger
Udviklingen i samfundet betyder, at grænser mellem kontinenter, lande og it-systemer brydes ned.	• Harmonisering af lovgivningen på privacy-området på nordisk og globalt plan

Skal man alene ved lov regulere eller skal der andre styringsmidler til?

Frem til nyere tid har der ikke været nogen tvivl om, at lovgivningen har en rolle at spille i reguleringen af informations- og kommunikationssamfundet og mere specifikt Internettet. Igennem de senere år er der dog opstået en erkendelse af, at eksisterende love og anden traditionel regulering ikke er tilstrækkelig til regulering af de forskellige konsekvenser af teknologien.

De problemstillinger, som knytter sig til konsekvenserne af teknologierne, er så komplekse, at specifik lovgivning målrettet disse ikke vil give mening. Den gængse opfattelse (også baseret på enkeltsager i medierne) er, at lovgivningen er mangelfuld i forhold til en "tilstrækkelig" beskyttelse af privatlivets fred for den enkelte borger. Der er derfor behov for supplement af lovgivning med andre styringsmidler.

Disse andre styringsmidler bliver dog også i stigende grad taget i anvendelse. Eksempler på andre styringsmidler kan være:

- Statslige oplysningskampagner til borgerne om privacy og teknologiernes muligheder og trusler.
- Standardisering af teknologier og herunder udbredelse af normer for teknologianvendelse.
- Anvendelse af kontraktstyring og opfølgende kontrol, når personfølsomme data og dataanvendelse outsources til private virksomheder.
- Økonomiske tilskud fra staten til private aktører på markedet som f.eks. ISP'ere og softwareleverandører.
- Statslig initiering og drift af samarbejder mellem aktører i markedet.
- Frivillige aftaler mellem aktører med betydning for privacy. Et eksempel herpå er det kodeks, som ISP'ere i Danmark har udarbejdet.

Fælles for alle disse styringsmidler er, at ingen af dem enkeltstående vil give "tilstrækkelig" beskyttelse af borgernes privacy, men må indgå i den palette af styringsmidler, der tages i anvendelse. Før tiltagene igangsættes, er det dog nødvendigt at foretage en afvejning af styrker og svagheder ved disse, samt om de har den ønskede effekt. Vurderingen bør ligeledes indeholde et tidsperspektiv, da nogle tiltag kan have den ønskede effekt på meget lang sigt, uden at den kan måles på kort sigt.

Initiativet til igangsættelse af handlinger kan komme fra såvel nationale som internationale myndigheder og organisationer samt fra private virksomheder og organisationer. Analyser og forhandlinger herom tager tid, og mange har også været i gang i flere år. Men mens tiden går, er borgernes privacy truet.

Sammenfatning

Politiske udfordringer	Løsninger
Eksisterende love og anden traditionel regulering er ikke tilstrækkelig til regulering af de forskellige konsekvenser af teknologien.	• Den eksisterende lovgivning skal suppleres og understøttes med andre styringsmidler.

Borgernes rettigheder i forhold til rigets sikkerhed

De seneste års vækst i antallet af terrorhandlinger, eller i hvert fald den øgede information til offentligheden omkring terrorhandlinger, har afstedkommet en øget indsats i overvågning og kontrol af alle borgere med det formål at identificere og straffe terrorister. Debatten er i dag i gang også i medierne og belyser bl.a. en problemstilling om, hvorvidt staten kan forudsætte befolkningens fulde tillid til styrkelse af overvågningen og kontrollen med borgerne med det mål at bekæmpe de kriminelle.

Flere medier i Danmark har kørt undersøgelser på, om borgerne kan og vil acceptere overvågning for at sikre den generelle sikkerhed. Ingen af disse undersøgelser er dog særlig valide, og resultaterne heraf derfor også blandede. I situationer, hvor terrorismens grusomme ansigt toner frem på samtlige nyhedsmedier, er alle ikke sene til at acceptere overvågningen og kontrollen. Disse skræmmescenarier har den indlysende virkning på os alle, at vi er tilbøjelige til at give køb på demokratiske rettigheder omkring privatlivets fred. Nogle vil mene, at det er nødvendigt og uundgåeligt i vores tid.

Når staten registrerer og opbevarer data omkring borgerne, har vi som borgere tillid til og forventer, at statsmagten ikke misbruger informationen eller "mister" kontrollen med data, så de kan misbruges.

Debatten bør også omhandle det forhold, at de organiserede kriminelle og terrorister, der ønsker at undgå overvågning, har mulighederne for dette ved at udnytte de teknologiske muligheder. Herved mister overvågningen sin fulde effekt og dermed en væsentlig del af rationalet - på bekostning af krænkelse af privatlivets fred for borgerne.

Vi har i delrapport 2 listet de teknologier, der i dag muliggør anonym adfærd og kommunikation f.eks. med kryptering. Disse teknologier er i dag i princippet mulige at anvende for alle, men forudsætter viden og kompetencer herom. Det er således muligt og lovligt også for kriminelle/terrorister/frihedskæmpere mv. at kommunikere på denne måde og således undgå at blive identificeret og opdaget. Det er endvidere ualmindeligt vanskeligt, hvis ikke praktisk umuligt, at forbyde eller hindre, at privatlivsfremmende teknologier benyttes af kriminelle, da disse teknologier udvikles og udbydes af globale intellektuelle communities uden for statsmagternes kontrolrum.

En omvendt situation, hvor staten ønsker at udbrede mere privatlivsfremmende teknologi, vil samtidig arbejde imod et eventuelt mål om øget overvågning.

Der er et politisk dilemma i, at ved at øge mulighederne for at bekæmpe kriminalitet ved udvidet overvågning, mindskes almindelige borgeres ret til at optræde anonymt og dermed etablere et privacy-rum.

Endelig er der afledt et dilemma omkring, hvilken fejlmargin man politisk vil tolerere. Det vil sige, at når overvågning og data kan sammenkøres af sagsbehandlere og it-systemer, vil der uundgåeligt fra tid til anden kunne blive begået en fejl og dermed draget en forkert slutning. Det kan således i nogen grad forventes, at "uskyldige" borgere f.eks. blacklistes i politiets og efterretningstjenestens registre, uden at de har mulighed for at vide det og redegøre for deres uskyld.

Sammenfatning

Politiske udfordringer	**Løsninger**
At etablere en overvågning og/eller kontrol, som effektivt og tilstrækkeligt opfylder målet.	• Løsning på disse to udfordringer ligger i afvejningen mellem borgernes ret til privacy og hensynet til rigets og borgernes sikkerhed, som kun kan løses ved en politisk beslutning.
Der findes i dag teknologi, som gør det muligt og lovligt, også for kriminelle/terrorister/frihedskæmpere m.fl., at kommunikere, uden at man bliver identificeret.	• Se ovenfor.
Udbredelse af PET-teknologier undergraver rationalet omkring øget overvågning for at kunne bekæmpe terrorisme mv.	• Der bør foretages omfattende effektvurdering af tiltag med betydning for privacy, før disse iværksættes. Tiltagene bør tillige vurderes ud fra politiske hensigter og mål samt samfundsøkonomiske konsekvenser.

Nordisk Ministerråd har bestilt og finansieret nærværende konsulentrapport.

- Rapporten er udarbejdet af Deloitte.

Deloitte. Enterprise Risk Services, Weidekampsgade 6, 2300 København S. Telefon: +45 36 10 20 30