JUSTITSMINISTERIET
Civil- og Politiafdelingen

Dato: 2. juli 2010
Kontor: Politikontoret
Sagsnr.: 2009-945-1473
Dok.: TTM41265

Notat om arbejdsgruppens overvejelser om indførelsen af en brugerregistrering af taletidskort

Indledning

1. Spørgsmålet om brugerregistrering af taletidskort har tidligere været overvejet. Den tværministerielle arbejdsgruppe om terrorbekæmpelse anbefalede således i rapporten *Det danske samfunds indsats og beredskab mod terror* fra oktober 2005, at det teknologiske område, hvor politiet ikke har nogen umiddelbar mulighed for at sammenholde brugeroplysninger med det enkelte kommunikationsapparat (taletidskort, internetcaféer mv.), elimineres eller – hvis dette ikke er muligt – reduceres i videst muligt omfang (anbefaling 16).

Som opfølgning på denne anbefaling – og i overensstemmelse med regeringens handlingsplan for terrorbekæmpelse fra november 2005 – nedsatte Justitsministeriet og Ministeriet for Videnskab, Teknologi og Udvikling en arbejdsgruppe med henblik på at afklare problemernes omfang og skitsere mulige løsninger.

Denne arbejdsgruppe anbefalede i sommeren 2006, at der ikke indføres et krav om brugerregistrering af taletidskort, idet arbejdsgruppen bl.a. vurderede, at mange taletidskort blev solgt i kioskmiljøet, hvor det ville være vanskeligt at håndhæve et krav om registrering af oplysninger om købere. Det ville endvidere ifølge arbejdsgruppen være ganske omkostningsfuldt for telebranchen at gennemføre et krav om indretning af tekniske systemer med henblik på brugeridentifikation.

2. Siden denne arbejdsgruppe i 2006 færdiggjorde sit arbejde har Politiets Efterretningstjeneste (PET) og det øvrige politi oplevet en betydelig stigning i de problemer, som brugen af uregistrerede taletidskort udgør i forbindelse med efterforskningen af sager om terrorisme og organiseret kriminalitet.

Slotsholmsgade 10
1216 København K.

Telefon 7226 8400
Telefax 3393 3510

www.justitsministeriet.dk
jm@jm.dk

Der ses således at være en stigende tendens til, at taletidskort bevidst bruges til at vanskeliggøre politiets efterforskning. PET har konstateret, at uregistrerede taletidskort nu optræder i stort set alle dets operationer og efterforskninger, ligesom det er Rigspolitiets erfaring, at uregistrerede taletidskort systematisk anvendes i forbindelse med organiseret kriminalitet – herunder bande- og rockerkriminalitet – som et middel til at unddrage sig politiets efterforskning.

Regeringen nedsatte på den baggrund i efteråret 2009 en arbejdsgruppe bestående af repræsentanter for Justitsministeriet, Videnskabsministeriet samt Rigspolitiet, PET og IT- og Telestyrelsen, der skal overveje, hvordan oplysninger om brugere af taletidskort, internetcaféer, gratis hotspots og internetadgang på biblioteker mv. kan registreres, så det sikres, at politiet har mulighed for at sammenholde oplysninger om brugeren med oplysninger om kommunikationsapparatet.

Efter kommissoriet skal arbejdsgruppen gennemgå og vurdere de tekniske muligheder for at registrere sådanne oplysninger, og i den forbindelse skal arbejdsgruppen inddrage erfaringer fra andre lande samt inddrage telebranchen i arbejdet.

På baggrund af overvejelserne skal arbejdsgruppen komme med anbefalinger om en mulig brugerregistreringsordning ved bl.a. taletidskort, og arbejdsgruppen skal i den forbindelse også belyse de økonomiske og administrative konsekvenser.

Udenlandske erfaringer

3. Arbejdsgruppen skal som anført ovenfor inddrage erfaringer fra andre lande i sit arbejde. Arbejdsgruppen har på den baggrund rettet henvendelse til en række lande, herunder Norge, Tyskland og Spanien, med henblik på at få oplyst, om de stiller krav om brugerregistrering af taletidskort, og i det omfang det er tilfældet, hvordan ordningen er indrettet.

Norge

Den norske telemyndighed Post- og Teletilsynet har oplyst, at der i Norge er en pligt til at registrere alle slutbrugere, herunder brugere af taletidskort. Pligten til brugerregistrering fremgår af § 6-2 i den norske forskrift om elektronisk kommunikationsnet og elektronisk kommunikationstjeneste (ekomforskriften), som er udstedt med hjemmel i den norske lov om elektronisk kommunikation (ekomloven).

Ifølge Post- og Teletilsynet er hovedkravet efter § 6-2 i ekomforskriften, at der foretages en entydig registrering af brugeren/ejeren, inden telefontjenesten kan benyttes. Ansvaret herfor ligger hos udbyderne.

Ekomforskriftens § 6-2 har følgende ordlyd:

> *§ 6-2. Informasjon om sluttbrukere*
>
> Tilbyder av offentlig telefontjeneste skal føre oversikt over enhver sluttbrukers navn, adresse og nummer/adresse for tjeneste. Oversikten skal inneholde opplysninger som muliggjør entydig identifisering av de registrerte og opplysninger som muliggjør geografisk lokalisering av de registrerte i forbindelse med nødanrop, jf. § 6-3 annet ledd og ekomloven § 2-6. Informasjon om offentlig betalingstelefon skal omfatte adresse.
>
> Tilbyder av offentlig telefontjeneste skal vederlagsfritt og før oppføring skjer, gi sluttbruker informasjon om formålet med offentlig tilgjengelig trykt eller elektronisk opplysningssystem der opplysninger om sluttbrukeren vil fremgå, og om mulig bruk av opplysningene som følge av søkemuligheter i elektroniske opplysningssystem.
>
> Sluttbruker skal vederlagsfritt kunne kontrollere, rette og trekke tilbake registrerte opplysninger. Sluttbrukere kan reservere seg helt eller delvis mot at informasjon om egne nummer, navn eller adresse utleveres til allmennheten. Tilbyder av offentlig telefontjeneste skal opplyse sluttbruker om at reservasjon mot oppføring i opplysningssystem kan gjøres vederlagsfritt.
>
> Sluttbruker skal etter anmodning få disponere hemmelig nummer.
>
> Tilbyder av opplysningssystem skal slette opplysninger om sluttbruker som har reservert seg mot offentliggjøring etter tredje og fjerde ledd fra offentlig tilgjengelig trykt eller elektronisk opplysningssystem ved første oppdatering.
>
> Uten forhåndssamtykke fra den registrerte kan opplysningssystem bare benyttes til søk etter informasjon på grunnlag av brukerens navn, adresse, nummer/adresse for tjeneste.
>
> Tilbyder av opplysningstjeneste skal sikre at opplysningssystemet er i overensstemmelse med personopplysningsloven og at det ikke gis opplysninger i strid med taushetsplikt.

Efter § 6-3 i ekomforskriften har udbyderne pligt til at registrere bl.a. fødselsdato eller organisationsnummer.

Ekomforskriftens § 6-3 har følgende ordlyd:

> § 6-3. Plikt til å utveksle nummeropplysningsinformasjon
>
> Tilbyder av offentlig telefontjeneste plikter på en objektiv, ikke-diskriminerende måte og til kostnadsorienterte priser å stille nummeropplysningsinformasjon etter § 6-2 til rådighet på forespørsel fra tilbydere av opplysningstjeneste, når informasjonen skal nyttes i nummeropplysningsvirksomhet. Nummeropplysningsvirksomhet omfatter ikke verdiøkende virksomhet i egen eller andres salgs- og markedsføringsøyemed til annen bruk enn nummeropplysning.
>
> Nummeropplysningsinformasjon som skal overføres etter første ledd er:
>
> 1. Unik ID; fødselsdato eller organisasjonsnummer
> 2. brukers etternavn, fornavn og mellomnavn for personlige brukere eller firmanavn. Når juridisk eier av abonnement og bruker ikke er den samme, skal bare brukers navn overføres
> 3. gatenavn eller postadresse
> 4. husnummer
> 5. postnummer
> 6. poststed
> 7. telefonnummer, herunder angivelse av hovednummer når dette er registrert eller meldt av sluttbruker
> 8. brukstype, det vil si om nummeret brukes til fasttelefon, mobiltelefon eller telefaks.
>
> Nummeropplysningsinformasjon om sluttbrukere som har reservert seg mot at informasjon om egne nummer, navn eller adresser utleveres til allmennheten etter § 6-2 tredje ledd, skal ikke overføres.

> Ved overføring af opplysninger skal det opplyses om nyoppføring, endring i eksisterende opplysninger og sletting av registrering. Sletting angis som endring av tidligere overførte opplysninger. Der unik identitet har flere nummer angis endring av nummer som sletting av eksisterende oppføring og ny oppføring.
>
> Avgiver og mottaker dekker egne kostnader ved tilrettelegging for overføring av opplysninger. Mottaker skal dekke kostnadene ved selve overføringen.
>
> Avgiver og mottaker skal sikre personopplysningenes kvalitet i forhold til behandlingsformålet. Dersom annet ikke er avtalt, skal oppdatert nummeropplysningsinformasjon utleveres en gang per virkedag i elektronisk form som masseopplysninger og være i samsvar med standardformatet ISO 8859-1.
>
> Plikter etter denne bestemmelsen innskrenker ikke sluttbrukers rettigheter fastsatt i eller i medhold av personopplysningsloven.

Post- og Teletilsynet har endvidere oplyst, at man senest ved et brev af 10. oktober 2006 har skrevet til udbyderne med henblik på at indskærpe kravene til registrering af brugere af taletidskort. Den nærmere indretning af procedurer til sikring af den rigtige identitet er imidlertid op til de enkelte udbydere.

På baggrund af oplysningerne fra Post- og Teletilsynet ses der umiddelbart i Norge at være to modeller til sikring af en entydig registrering. Den første indebærer, at der ringes til udbyderens kundeservice og angives personoplysninger, der herefter sammenholdes med oplysningerne i folkeregisteret. Teknisk fungerer denne model således, at der indtastes en kode på telefonen, hvorefter der alene kan ringes til udbyderens kundeservice. Når kundeservice herefter har registreret de rigtige oplysninger, aktiveres telefonen.

Den anden model går ud på, at kunden enten over for udbyderen eller over for sælgeren af taletidskortet legitimerer sig. Denne model tænkes navnlig anvendt af de kunder, som ikke er registreret i folkeregisteret.

Post- og Teletilsynet har oplyst, at telebranchen i første omgang var tilbageholdende over for pligten til at registrere taletidskunder, idet det blev gjort gældende, at det ville være forbundet med store omkostninger, og at en registrering ikke ville være muligt at gennemføre på grund af de mange forskellige salgssteder for sådanne kort. Post- og Teletilsynet oplyser dog, at det system, der siden er udviklet, vurderes at indebære en acceptabel balance mellem på den ene side omkostningerne og på den anden side registreringspligten.

Den norske efterretningstjeneste (PST) har vedrørende deres erfaringer med den norske ordning oplyst, at registreringspligten er en stor hjælp i det daglige arbejde, selv om der stadig er mulighed for at snyde med legitimationen, og selv om udenlandske taletidskort fortsat kan anvendes i Norge uden at være registreret.

Tyskland

De tyske myndigheder har oplyst, at udbydere efter tysk lovgivning er forpligtet til at indsamle og gemme oplysninger om slutbrugere, herunder brugere af taletidskort, før et telefonnummer aktiveres med henblik på at kunne give myndighederne adgang til disse oplysninger. Den nærmere regulering af forpligtelsen findes i § 111 i den tyske telelov (Telekommunikationsgesetz), der også opregner, hvilke oplysninger der skal indsamles og gemmes. Det drejer sig bl.a. om navn, adresse og fødselsdato.

§ 111 i den tyske telelov har følgende ordlyd:

> (1) Wer geschäftsmäßig Telekommunikationsdienste erbringt oder daran mitwirkt und dabei Rufnummern oder andere Anschlusskennungen vergibt oder Telekommunikationsanschlüsse für von anderen vergebene Rufnummern oder andere Anschlusskennungen bereitstellt, hat für die Auskunftsverfahren nach den §§ 112 und 113
> 1. die Rufnummern und anderen Anschlusskennungen,
> 2. den Namen und die Anschrift des Anschlussinhabers,
> 3. bei natürlichen Personen deren Geburtsdatum,
> 4. bei Festnetzanschlüssen auch die Anschrift des Anschlusses,
> 5. in Fällen, in denen neben einem Mobilfunkanschluss auch ein Mobilfunkendgerät überlassen wird, die Gerätenummer dieses Gerätes sowie
> 6. das Datum des Vertragsbeginns
> vor der Freischaltung zu erheben und unverzüglich zu speichern, auch soweit diese Daten für betriebliche Zwecke nicht erforderlich sind; das Datum des Vertragsendes ist bei Bekanntwerden ebenfalls zu speichern. Satz 1 gilt auch, soweit die Daten nicht in Teilnehmerverzeichnisse (§ 104) eingetragen werden. Die Verpflichtung zur unverzüglichen Speicherung nach Satz 1 gilt hinsichtlich der Daten nach Satz 1 Nr. 1 und 2 entsprechend für denjenigen, der geschäftsmäßig einen öffentlich zugänglichen Dienst der elektronischen Post erbringt und dabei Daten nach Satz 1 Nr. 1 und 2 erhebt, wobei an die Stelle der Daten nach Satz 1 Nr. 1 die Kennungen der elektronischen Postfächer und an die Stelle des Anschlussinhabers nach Satz 1 Nr. 2 der Inhaber des elektronischen Postfachs tritt. Wird dem Verpflichteten nach Satz 1 oder Satz 3 eine Änderung bekannt, hat er die Daten unverzüglich zu berichtigen; in diesem Zusammenhang hat der nach Satz 1 Verpflichtete bisher noch nicht erhobene Daten zu erheben und zu speichern, sofern ihm eine Erhebung der Daten ohne besonderen Aufwand möglich ist. Für das Auskunftsverfahren nach § 113 ist die Form der Datenspeicherung freigestellt.
> (2) Bedient sich der Diensteanbieter nach Absatz 1 Satz 1 oder Satz 3 eines Vertriebspartners, hat der Vertriebspartner die Daten nach Absatz 1 Satz 1 und 3 unter den dort genannten Voraussetzungen zu erheben und diese sowie die nach § 95 erhobenen Daten unverzüglich dem Diensteanbieter zu übermitteln; Absatz 1 Satz 2 gilt entsprechend. Satz 1 gilt auch für Daten über Änderungen, soweit sie dem Vertriebspartner im Rahmen der üblichen Geschäftsabwicklung zur Kenntnis gelangen.
> (3) Für Vertragsverhältnisse, die am Tage des Inkrafttretens dieser Vorschrift bereits bestehen, müssen Daten im Sinne von Absatz 1 Satz 1 oder Satz 3 außer in den Fällen des Absatzes 1 Satz 4 nicht nachträglich erhoben werden.
> (4) Die Daten sind mit Ablauf des auf die Beendigung des Vertragsverhältnisses folgenden Kalenderjahres zu löschen.
> (5) Eine Entschädigung für die Datenerhebung und -speicherung wird nicht gewährt.

Ifølge de tyske myndigheder kan registreringen enten ske i forbindelse med købet i udbyderens elektroniske kundesystem, eller – for så vidt angår forudbetalte taletidskort, der købes i supermarkeder mv. – via en hotline til udbyderen eller på dennes hjemmeside.

De tyske myndigheder har peget på, at kvaliteten af de indsamlede oplysninger om taletidskunder ikke altid er den bedste. Dette skyldes ifølge de tyske myndigheder, at udbyderne ikke er forpligtet til at indsamle og gemme oplysningerne på baggrund af et officielt identifikationspapir. Udbyderne kan forlange at se et officielt identifikationspapir, men de er ikke forpligtet til at gøre det.

Spanien
De spanske myndigheder har oplyst, at udbyderne siden 2007 har været forpligtet til at registrere brugere af taletidskort. Udbyderne skal således registrere navn og nationalitet på brugerne i en logbog, som bl.a. politiet herefter har adgang til. Ordningen har efter det oplyste ikke nogen betydning for aktiveringen af telefonen.

Arbejdsgruppens overvejelser
Politimæssigt behov
4. Arbejdsgruppen konstaterer, at brugen af taletidskort udgør et stigende problem for PET og det øvrige politi, idet taletidskort i dag bevidst bruges til at vanskeliggøre politiets efterforskning. Det gælder såvel i sager om terrorisme, som i sager om organiseret kriminalitet.

Arbejdsgruppen har i den forbindelse lagt vægt på, at PET har oplyst, at uregistrerede taletidskort i dag optræder i stort set alle PET's operationer og efterforskninger, ligesom Rigspolitiet har oplyst, at uregistrerede taletidskort også systematisk anvendes i forbindelse med organiseret kriminalitet – herunder bande- og rockerkriminalitet – som et middel til at unddrage sig politiets efterforskning.

Det er på den baggrund arbejdsgruppens opfattelse, at indførelsen af et krav om brugerregistrering vil kunne indebære en række klare fordele for politiets mulighed for at efterforske sager om terrorisme og organiseret kriminalitet.

Arbejdsgruppen er i den forbindelse opmærksom på, at det – uanset et krav om brugeregistrering – fortsat i et vist omfang vil være muligt at omgå registreringen. Dette ændrer imidlertid ikke ved, at en brugerregistrering efter arbejdsgruppens opfattelse vil være en fordel for politiet, idet en sådan ordning alt andet lige vil reducere de kriminelles mulighed for at gemme sig bag anonyme taletidskort.

Afvejning

5. Arbejdsgruppen har overvejet, om de fordele, som en registreringsordning vil indebære for politiets muligheder for at efterforske sager om terrorisme og organiseret kriminalitet, står i et rimeligt forhold til de byrder, som en registreringsordning vil påføre telebranchen.

Spørgsmålet om byrderne for telebranchen vil blive undersøgt nærmere, blandt andet vil der blive indhentet erfaringer fra udlandet, ligesom eventuelle konsekvenser for markedet for taletidskort skal klarlægges. Telebranchen bør efter arbejdsgruppens opfattelse inddrages i spørgsmålet om byrderne.

Krav til en registreringsordning

Arbejdsgruppen finder, at en afgørende forudsætning for en registreringsordning – også for så vidt angår spørgsmålet om omkostninger – må være, at ordningen kan bruges som et effektivt redskab for politiet i forbindelse med efterforskningen.

En ordning bør derfor efter arbejdsgruppens opfattelse indrettes på en sådan måde, at man i videst muligt omfang kan undgå brugen af falske identiteter. Dette stiller dels krav til, hvornår oplysningerne skal være registreret, dels krav til oplysningernes kvalitet.

Det bør således indgå som en afgørende forudsætning i en brugerregistreringsordning, at et taletidskort ikke kan aktiveres, før oplysningerne om taletidskortkunden er registreret hos teleudbyderen. Identifikationen bør endvidere være entydig og bygge på oplysninger, der forud for eller samtidig med aktiveringen kan verificeres med henblik på at sikre rigtigheden af dem.

Den forudgående eller samtidige verificering vil endvidere minimere risikoen for, at personer, hvis identitet er blevet misbrugt, uden skyld bliver gjort til genstand for en politimæssig efterforskning.

Med henblik på at sikre rigtigheden af oplysningerne må der efter arbejdsgruppens opfattelse kunne stilles krav om, at de oplysninger, der afgives af kunden, som udgangspunkt enten skal kunne sammenholdes med oplysningerne i Det Centrale Personregister eller verificeres via et betalingskort.

Efter det for arbejdsgruppen oplyste foretager hovedparten af teleudbyderne allerede i dag kontrol af de oplysninger, der afgives af den enkelte

kunde i forbindelse med indgåelsen af en abonnementsaftale. Denne kontrol gennemføres i praksis enten i forbindelse med kundens anvendelse af et betalingskort eller ved, at den pågældende – udover oplysninger om navn og adresse mv. – oplyser sit personnummer, hvorefter teleudbyderen via Det Centrale Personregister sammenholder personnummeret med de øvrige kundeoplysninger.

Det er arbejdsgruppens opfattelse, at teleudbyderne vil kunne foretage den fornødne entydige identifikation af taletidskortkunden (jf. ovenfor) ved fremover også at anvende sådanne eller lignende procedurer i forbindelse med køb af taletidskort.

I det omfang det ikke er muligt for teleudbyderen at verificere kundens identitet via et betalingskort eller ved at sammenholde de oplysninger, der afgives af kunden, med oplysningerne i Det Centrale Personregister, må det på anden måde sikres, at der er tale om rigtige oplysninger. Det kan f.eks. ske ved fysisk fremvisning af billedlegitimation.

6. Det er samtidig arbejdsgruppens opfattelse, at det er mest hensigtsmæssigt at overlade det til de enkelte udbydere at indrette sig på en sådan måde, at der opnås størst mulig sikkerhed omkring de registrerede oplysningers rigtighed.

Arbejdsgruppen vil derfor ikke anbefale en bestemt model for registrering af brugeroplysninger. De enkelte udbydere kan således have forskellige sagsgange i forbindelse med administrationen af deres taletidskort, som gør, at en løsning, der passer på en udbyder, ikke passer på en anden. I den forbindelse spiller det naturligvis også en rolle, om der er tale om taletidskort, der sælges via udbyderens hjemmeside, i en af dennes butikker eller f.eks. i supermarkeder.

En registreringsordning bør derfor ikke gennemføres ved fastsættelse af regler, der indebærer bestemte tekniske krav til, hvordan teleudbyderne skal opfylde forpligtigelsen. Det bør i stedet overlades til de enkelte udbydere nærmere at indrette sig.

Hvilke oplysninger?

7. Arbejdsgruppen har også overvejet, om det nærmere bør præciseres, hvilke oplysninger udbyderne skal registrere i forhold til deres taletidkortkunder. Det følger allerede af lov om konkurrence- og forbrugerforhold på telemarkedet, lov nr. 780 af 28. juni 2007 (teleloven) § 34, stk. 2,

som udmøntet ved bekendtgørelse om nummeroplysningsdata, nr. 731 af 30. juni 2008, at udbydere bl.a. skal registrere navn og adresse på en abonnementskunde. Dette gælder dog ikke for anonyme abonnementer, som for eksempel forudbetalte taletidskort. Derimod stilles der ikke – som tilfældet er i Norge og Tyskland – krav om, at fødselsdato registreres.

Det vil efter arbejdsgruppens opfattelse være nærliggende også i forhold til taletidskortkunderne at tage udgangspunkt i de oplysninger, som udbyderne er forpligtet til at registrere i forhold til deres abonnementskunder.

Det er imidlertid vigtigt, at der samtidig etableres en pligt for udbyderne til at sikre, at der er overensstemmelse mellem abonnementskundens egentlige navn og adresse og de oplysninger kunden angiver til udbyderen herom i forbindelse med oprettelsen af abonnementet.

Politiet har i dag direkte adgang til den såkaldte nummeroplysningstjeneste (118-databasen), og det er denne nummeroplysningstjeneste, som politiet i dag bruger, når der f.eks. ønskes oplysninger om, hvem et telefonnummer tilhører.

Denne database indeholder oplysninger om alle telefonnumre samt – i forhold til abonnementsforhold – også oplysninger om kunder herunder navn og adresse. I forhold til numre, der anvendes til forudbetalte taletidskort, indeholder databasen således alene oplysninger om disses anvendelse, jf. § 5, stk. 3, i bekendtgørelse nr. 701 af 26. juni 2008 om forsyningspligtydelser.

Det bør efter arbejdsgruppens opfattelse overvejes, om en ordning for brugerregistrering af taletidskort kan kobles sammen med den eksisterende nummeroplysningstjeneste (118-databasen), der som beskrevet allerede indeholder oplysninger om bl.a. de telefonnumre, der er knyttet til de enkelte taletidskort.

Ved at koble en brugeregistreringsordning af taletidskort på den eksisterende nummeroplysningstjeneste sikres det, at der fortsat kun vil være en indgang for politiet til oplysninger om, hvem et telefonnummer tilhører og omvendt. Hertil kommer, at der efter arbejdsgruppens opfattelse også kan være nogle fordele for branchen forbundet med, at der bygges videre på en kendt ordning.

Sammenfatning

8. Sammenfattende er det arbejdsgruppens opfattelse,

- at der er et politifagligt behov for at sikre identiteten på brugere af taletidskort;
- at en ordning for brugeregistrering bør indrettes således, at den sikrer en tilpas balance mellem de efterforskningsmæssige fordele for politiet og byrderne for telebranchen;
- at en ordning i videst mulige omfang bør sikre, at brugen af falske identiteter undgås; og
- at den nærmere tekniske løsning overlades til telebranchen.

JUSTITSMINISTERIET
Civil- og Politiafdelingen

Dato: 17. juni 2011
Kontor: Politikontoret
Sagsnr.: 2009-945-1473
Dok.: JJA40456

Notat om arbejdsgruppens overvejelser om indførelsen af en ordning med registrering af brugere af internetcaféer, hotspots og internetadgang på biblioteker mv.

Indhold

Slotsholmsgade 10
1216 København K.

Telefon 7226 8400
Telefax 3393 3510

www.justitsministeriet.dk
jm@jm.dk

1. Baggrund

I sit afsnit om efterforskningsredskaber på teleområdet anbefalede den tværministerielle arbejdsgruppe om terrorbekæmpelse (Bernstein-udvalget) i oktober 2005, at det teknologiske område, hvor politiet ikke har nogen umiddelbar mulighed for at sammenholde brugeroplysninger med det enkelte kommunikationsapparat (taletidskort, internetcaféer mv.), elimineres eller – hvis dette ikke er muligt – reduceres i videst muligt omfang (anbefaling 16).

Som opfølgning på denne anbefaling – og i overensstemmelse med regeringens handlingsplan for terrorbekæmpelse fra november 2005 – nedsatte Justitsministeriet og Ministeriet for Videnskab, Teknologi og Udvikling en arbejdsgruppe, som fik til opgave at afklare problemernes omfang og skitsere mulige løsninger.

Arbejdsgruppen afsluttede sit arbejde i sommeren 2006. Arbejdsgruppen fandt bl.a., at oplysninger om identiteten på brugere af internetcaféer kan være af væsentlig efterforskningsmæssig betydning.

Arbejdsgruppen anbefalede på den baggrund, at ejere og administratorer af internetcaféer forpligtedes til at registrere oplysninger om identiteten på deres kunder.

Arbejdsgruppen fandt imidlertid ikke, at man på daværende tidspunkt havde tilstrækkeligt grundlag for at anbefale en brugerregistreringsordning med hensyn til trådløse net, der på offentligt tilgængelige steder stilles til rådighed for brugere (såkaldte hotspots) og internetadgang på biblioteker mv. Arbejdsgruppen anbefalede derfor, at der blev arbejdet videre med at afklare omfanget af de problemer, der knytter sig til internetadgang via hotspots og biblioteker, og skitsere mulige løsninger på problemerne.

Siden arbejdsgruppen færdiggjorde sine overvejelser i sommeren 2006, har bl.a. en stigende udbredelse af hotspots og en øget tilgængelighed af andre "anonyme" former for internetkommunikation medført tiltagende problemer for politiets – herunder Politiets Efterretningstjenestes – muligheder for at efterforske sager om bl.a. terrorisme og organiseret kriminalitet, hvor indgreb i meddelelseshemmeligheden ofte er et afgørende efterforskningsredskab.

Regeringen nedsatte på denne baggrund i november 2009 en ny arbejdsgruppe bestående af repræsentanter fra Justitsministeriet og Ministeriet for Videnskab, Teknologi og Udvikling samt Rigspolitiet, Politiets Efterretningstjeneste og IT- og Telestyrelsen. Arbejdsgruppen fik til opgave at overveje, hvordan oplysninger om brugere af internetcaféer, gratis hotspots og internetadgang på biblioteker mv. kan registreres, så det sikres, at politiet har mulighed for at sammenholde oplysninger om brugeren med oplysninger om kommunikationsapparatet. Arbejdsgruppen blev endvidere anmodet om at belyse økonomiske og administrative konsekvenser af en mulig registreringsordning.

Det er i kommissoriet forudsat, at arbejdsgruppen inddrager telebranchen i arbejdet.

2. Forskellige former for internetadgang

Det er overordnet muligt at skaffe sig adgang til internettet via enten kablet internetadgang eller mobilt bredbånd.

Ved en *kablet internetadgang* etableres adgangen til internettet via et internetstik, som er indlagt på en fysisk lokalitet. For at opnå adgang til internettet skal en computer tilsluttes internetstikket. Dette kan enten gøres via et kabel mellem computeren og internetstikket eller via en trådløs router, som er tilsluttet stikket, jf. nærmere herom nedenfor.

Ved *mobilt bredbånd* skabes adgangen til internettet via luftbårne signaler, der sendes mellem en given computer eller mobiltelefon og et mobilselskabs sendemaster. Mobilt bredbånd forudsætter således ikke, at computeren direkte eller via en router tilsluttes et internetstik. Mobilt bredbånd kan derfor anvendes alle steder, hvor der kan sendes og modtages signaler fra et mobilselskabs sendemaster. Det mobile bredbånd til computere ligger typisk på en USB-nøgle i form af et USB-modem, som skal

isættes computeren for at skabe kontakt til en sendemast og derigennem til internettet.

Tal fra IT- og Telestyrelsen viser, at der 2. halvår 2010 fandtes 799.000 abonnementer på mobilt bredbånd og 2.642.000 mobiltelefonabonnementer anvendt til internetadgang.

Opgørelsen vedrørende mobiltelefonabonnementer anvendt til internetadgang omfatter dels såkaldte tillægsabonnementer, som indeholder særlige vilkår om benyttelse af internettet til et fast afregnet beløb, dels standardabonnementer, som ikke indeholder særlige vilkår herom, men hvor det kan konstateres, at der er etableret adgang til internettet inden for de seneste tre måneder forud for IT- og Telestyrelsens opgørelsestidspunkt.

Ved *trådløse net* gøres det via en router muligt for flere brugere at dele en kablet internetadgang eller et mobilt bredbånd. Routeren udsender inden for et afgrænset område et internetsignal, som herefter kan opfanges af computere eller mobiltelefoner, der har den hardware og software, som er nødvendig for at modtage routerens signal. Anvendelsen af trådløse net kan via adgangskoder begrænses til en bestemt brugerkreds. Trådløse net anvendes i dag i mange private hjem. Herudover er der opstillet trådløse net på en lang række offentligt tilgængelige steder (såkaldte hotspots) eksempelvis på cafeer, på hoteller og i offentlige transportmidler, ligesom der tilbydes reklamefinansieret trådløst net i form af bynet i en række afgrænsede byområder.

På hjemmesiden www.openwifi.dk, som indeholder en oversigt over danske hotspots, var der medio maj 2011 registreret 2.263 offentligt tilgængelige hotspots og bynet.

De senere års eksplosive udvikling i borgernes anvendelse af internet har sammen med en øget generel teknologianvendelse betydet, at tjenester, der er baseret på, at der kan opnås adgang til internettet overalt (såkaldte *nomadiske tjenester*), vinder frem. Eksempelvis vurderes det, at betaling for varer og tjenesteydelser via mobile enheder vil udvikle sig markant inden for de kommende år. Denne tendens underbygges af en stigende udbredelse af bl.a. hotspots i byerne, bynet og mobilt internet, som skaber mulighed for, at brugerne kan være online hvor som helst.

IT- og Telestyrelsen har opgjort, at pr. 30. juni 2010 var mobilt bredbånd eller trådløst net tilgængeligt i omkring 99 pct. af Danmark.

3. Politiets efterforskning i forhold til internetkommunikation

I det omfang betingelserne herfor er opfyldt, kan politiet, herunder Politiets Efterretningstjeneste, gøre brug af en række tvangsindgreb med henblik på at skaffe sig adgang til en mistænkts kommunikation på internettet. Det drejer sig bl.a. om aflytning af mistænktes internetforbindelse (retsplejelovens § 780, stk. 1, nr. 1), indhentning af loggede data hos mistænktes internetudbyder (retsplejelovens § 780, stk. 1, nr. 3) og dataaflæsning af den mistænktes computer (retsplejelovens § 791 b). Herudover kan der efter omstændighederne foretages ransagning – eventuelt hemmelig ransagning – af mistænktes computer i medfør af bestemmelserne i retsplejelovens § 793, stk. 1, og § 799, stk. 1.

Teknisk har politiet som udgangspunkt mulighed for at anvende alle de ovennævnte efterforskningsmuligheder, uanset om en mistænkts internetkommunikation foregår via kabel, mobilt bredbånd eller trådløst net.

Uanset internetkommunikationens form vil de nævnte efterforskningsredskaber kunne rettes mod den IP-adresse, som internetadgangen er knyttet op på, ligesom det i forbindelse med efterforskningen vil kunne være muligt at fastslå "identiteten" i form af en MAC- (Media Access Control) adresse på f.eks. netkortet i den computer, der kommunikeres fra. Det vil imidlertid alene være muligt at knytte en faktisk person op på den pågældende kommunikation, hvis personens identitet er blevet registreret i tilknytning til MAC-adressen, IP-adressen eller i forbindelse med den konkret etablerede adgang til internettet, og de registrerede oplysninger i øvrigt er tilgængelige.

Mens der i praksis altid vil være registreret oplysninger om en faktisk person eller virksomhed i tilknytning til en kablet forbindelse og typisk også på et mobilt bredbånd, vil det kun undtagelsesvis blive registreret, hvilke faktiske personer der gør brug af en internetadgang gennem et (åbent) trådløst net.

Typisk vil bynet og offentlige hotspots være stillet gratis til rådighed (enten af offentlige myndigheder eller som en accessorisk ydelse til eksempelvis transport- eller restaurationsvirksomhed) eller være baseret på en forudgående betaling, eksempelvis over "telefonregningen", hvilket i princippet kan bestå i et træk på taletiden på et taletidskort uden ID-registrering. I sådanne situationer vil der ikke være samme incitament for udbyderen til at sikre identifikation af brugerne, som i tilfælde hvor der

efterfølgende skal betales for tjenesten. I den udstrækning brugeren overhovedet skal afgive identitetsoplysninger, vil de afgivne oplysninger således typisk ikke blive gjort til genstand for en nærmere validering.

Der kan ligeledes forekomme tilfælde, hvor en kablet internetforbindelse anvendes af flere brugere, og hvor det derfor er vanskeligt at fastslå den enkelte brugers identitet. Dette kan eksempelvis være tilfældet på en internetcafe, et bibliotek eller på en arbejdsplads, hvor de ansatte via deres arbejdscomputere har adgang til internettet. Hvor der til den kablede forbindelse er knyttet flere computere, vil det efter omstændighederne være muligt at adskille kommunikation fra de enkelte computere fra hinanden, men det vil ofte være vanskeligt efterfølgende at fastlægge identiteten på brugerne, idet der ikke generelt sker en valideret registrering af brugerens identitet. De fleste virksomheder registrerer dog, hvilke arbejdscomputere eller brugerkonti der er tildelt den enkelte medarbejder, og politiet vil derfor (hvis sagens karakter ikke taler imod, at der rettes henvendelse til en arbejdsgiver) derigennem kunne få oplyst identiteten på brugeren.

Endelig udbydes mobilt bredbånd i dag også i en form, som i det væsentlige svarer til uregistrerede taletidskort for så vidt angår mobiltelefoni. Denne form for mobilt bredbånd er således baseret på, at brugeren køber et USB-modem, som indeholder software med en given mængde internettrafik eller fri trafik i en given periode. Når den mængde trafik, der er betalt for, er opbrugt, lukkes for adgangen til internettet. USB-modemmet kan købes i detailhandlen, uden at der stilles krav om registrering af køberens identitet.

4. Logning af oplysninger om teletrafik

4.1. Teleloven

Teleloven indeholder en række krav til udbydere af elektroniske kommunikationsnet eller -tjenester. Med udtrykket *"udbyder"* forstås den, som med et kommercielt formål stiller produkter, elektroniske kommunikationsnet eller -tjenester omfattet af teleloven til rådighed for andre, jf. telelovens § 2, nr. 1.

Teleloven indeholder imidlertid ingen regler for parter, der på ikke-kommercielt grundlag stiller internetadgang til rådighed, f.eks. via et ikke-kommercielt hotspot eller på et bibliotek.

Ved vurderingen af om net eller tjenester stilles til rådighed på kommercielt eller ikke-kommercielt grundlag, lægges der navnlig vægt på, om der skal betales – direkte eller indirekte – for at bruge internetadgangen, eller om opsætningen i øvrigt er foretaget for at opnå en fortjeneste.

Efter telelovens § 10, stk. 1, nr. 1, gælder der en række forpligtelser for udbydere af elektroniske kommunikationsnet eller -tjenester til slutbrugere. Udbyderne skal bl.a. uden afgift for staten sikre, at det tekniske udstyr og de tekniske systemer, de anvender, er indrettet således, at politiet kan få adgang til oplysninger om teletrafik og til at foretage indgreb i meddelelseshemmeligheden i form af historisk teleoplysning og historisk udvidet teleoplysning, fremadrettet teleoplysning og fremadrettet udvidet teleoplysning, aflytning og teleobservation, jf. retsplejelovens kapitel 71 og 74, herunder, for så vidt angår fremadrettet teleoplysning og udvidet teleoplysning, at politiet kan få adgang, umiddelbart efter at disse oplysninger registreres.

4.2. Retsplejeloven

Efter retsplejelovens § 786, stk. 4, påhviler det udbydere af telenet eller teletjenester at foretage registrering og opbevaring i 1 år af oplysninger om teletrafik til brug for efterforskning og retsforfølgning af strafbare forhold.

Hensigten med bestemmelsen er at sikre, at de pågældende oplysninger om teletrafik findes og er tilgængelige, hvis der bliver brug for dem.

Indhentelse af oplysninger om teletrafik i forbindelse med efterforskning og retsforfølgelse af kriminalitet udgør et indgreb i meddelelseshemmeligheden, og politiets adgang til at få udleveret sådanne oplysninger, som en udbyder har registreret og opbevaret, reguleres derfor af reglerne om indgreb i meddelelseshemmeligheden i retsplejelovens kapitel 71 samt eventuelt også af reglerne i kapitel 74 om beslaglæggelse og edition. Det betyder bl.a., at indhentelse af oplysninger om teletrafik som udgangspunkt kun kan foretages efter rettens forudgående kendelse.

4.3. Logningsbekendtgørelsen

Efter § 1 i logningsbekendtgørelsen skal udbydere af elektroniske kommunikationsnet eller -tjenester til slutbrugere foretage registrering og opbevaring af oplysninger om teletrafik, der genereres eller behandles i ud-

byderens net, således at disse oplysninger vil kunne anvendes som led i efterforskning og retsforfølgning af strafbare forhold.

Udtrykket "udbyder" i logningsbekendtgørelsen skal forstås i overensstemmelse med samme udtryk i telelovens § 2, nr. 1. Det betyder således, at alle parter, der på kommercielt grundlag stiller net eller tjenester til rådighed for slutbrugere, skal foretage registrering og opbevaring af en række oplysninger.

Da logningsforpligtelsen efter de gældende regler alene påhviler de *kommercielle* udbydere af kommunikationsnet mv., vil bl.a. en række offentlige myndigheder og institutioner ikke være omfattet heraf. Det gælder bl.a. biblioteker, hospitaler, universiteter og folkeskoler, der på ikke-kommercielt grundlag stiller net eller tjenester til rådighed for eksterne parter (lånere, patienter, studerende mv.).

Det udelukker imidlertid ikke, at der med afsæt i logningsreglerne vil kunne tilvejebringes internetoplysninger, der hidrører fra biblioteker, hospitaler mv. Da eksempelvis biblioteker ikke er udbydere i telelovens forstand, anses biblioteket som *slutbruger* i lovens og bekendtgørelsens forstand, hvorfor den udbyder, der leverer internetadgangen til bibliotekerne, er forpligtet til at logge bibliotekets ind- og udgående kommunikation.

Logningsforpligtelsen vil imidlertid i disse tilfælde alene omfatte teletrafikken ind og ud af den pågældende institution mv., men derimod ikke kommunikationen fra den enkelte bruger eller den enkelte computer mv.

I den udstrækning parter registrerer og opbevarer oplysninger om teletrafik uden at være forpligtede hertil efter logningsbekendtgørelsen, vil politiet på baggrund af retsplejelovens almindelige regler om indgreb i meddelelseshemmeligheden kunne få adgang til disse oplysninger i samme udstrækning, som hvis oplysninger blev opbevaret på baggrund af en forpligtelse til logning.

4.4. Logningsdirektivet

Størsteparten af logningsbekendtgørelsens bestemmelser gennemfører logningsdirektivet – EU's direktiv nr. 24 af 15. marts 2006 om lagring af data genereret eller behandlet i forbindelse med tilvejebringelse af

offentligt tilgængelige elektroniske kommunikationstjenester eller elektroniske kommunikationsnet – i dansk ret.

Det fremgår af direktivets artikel 1, at formålet med direktivet er at harmonisere medlemsstaternes bestemmelser om de pligter, der er pålagt "udbydere af offentligt tilgængelige elektroniske kommunikationstjenester eller af et offentligt kommunikationsnet", for så vidt angår lagring af visse data, der genereres eller behandles af de pågældende, med henblik på at sikre, at der er adgang til disse data i forbindelse med efterforskning, afsløring og retsforfølgning af grov kriminalitet som defineret af de enkelte medlemsstater i deres nationale lovgivning.

Logningsdirektivet indeholder en relativt detaljeret angivelse af de oplysninger, der skal lagres i medfør af direktivet. Derimod indeholder direktivet ikke en nærmere definition af udbyderbegrebet. Den præcise fastlæggelse af udbyderbegrebet er således overladt til national ret.

Logningsdirektivet er et minimumsdirektiv, hvilket indebærer, at direktivet alene fastsætter, hvilken regulering de enkelte medlemsstater som minimum er forpligtede til at gennemføre. Direktivet er således ikke til hinder for, at medlemsstaterne fastsætter regler, som er mere vidtgående end direktivet.

Kommissionen har den 18. april 2011 afgivet en evalueringsrapport om logningsdirektivet. Kommissionen konkluderer i rapporten bl.a., at datalogning er et nyttigt værktøj for de strafferetlige systemer og for retshåndhævelsen i EU.

Kommissionen anfører dog samtidig, at direktivet på visse områder kun i begrænset omfang har formået at skabe en harmonisering af medlemsstaternes logningsregler.

På den baggrund vil Kommissionen foretage en revision af logningsdirektivet og i lyset heraf foreslå nye regler på området.

5. Brugerregistrering

I det omfang udbydere af kommunikationsnet mv. er omfattet af telelovens udbyderbegreb (jf. ovenfor), vil de pågældende være forpligtigede til at registrere og opbevare oplysninger om teletrafik. Udbyderne er imidlertid alene forpligtede til at foretage registrering og opbevaring af

oplysninger om teletrafik, der – uafhængigt af logningsreglerne – genereres eller behandles i de pågældendes net, jf. logningsbekendtgørelsens § 1.

I den udstrækning en udbyder behandler oplysninger om identiteten på brugerne, som det eksempelvis er tilfældet i forbindelse med etablering af abonnementsforhold, vil disse oplysninger skulle registreres og opbevares, jf. logningsbekendtgørelsens § 5, stk. 2.

I praksis vil udbydere af internetadgang på eksempelvis internetcaféer eller via hotspots imidlertid sjældent have behov for at generere eller behandle oplysninger om identiteten på brugerne i deres net, hvilket betyder, at sådanne oplysninger som udgangspunkt ikke bliver registreret og opbevaret.

Tilsvarende vil der normalt alene være anledning for udbyderne til at søge en eventuel identitetsoplysning valideret, hvis der efterfølgende skal kunne opkræves betaling for ydelsen (jf. også ovenfor under pkt. 3).

6. Det politimæssige behov for brugerregistrering

Den politimæssige interesse i at kunne fastlægge identiteten på personer, der kommunikerer via internettet, er tosidet. En sammenkobling af sikre identitetsoplysninger og en given kommunikation vil således være af afgørende betydning, dels i forbindelse med kortlægning af en kendt målpersons kommunikation, dels i forbindelse med fastlæggelse af identiteten på afsendere eller modtagere af mistænkelig kommunikation, som politiet har fået kendskab til i forbindelse med en konkret efterforskning.

Den politi- og efterforskningsmæssige indsats udfordres grundlæggende af, at det ikke længere er tilstrækkeligt at iværksætte indgreb mod en målpersons hjemmeadresse og bopæl, hvor al kommunikationsudstyr tidligere var forankret, og tele- og internetselskaberne havde en fast adresse, hvorfra en given persons datakommunikation udgik.

Den politimæssige analyseopgave forbundet med fastlæggelse af en persons kommunikation vil ofte basere sig på nettrafik fra flere udbydere, ligesom identifikationen af en person på tværs af flere net kan være særdeles kompliceret. Hvis en bruger kommunikerer via en trådløs in-

ternetforbindelse, og den pågældende eksempelvis bevæger sig fra et område, der er dækket af ét hotspot, til et område, der er dækket af et andet, vil den pågældende som udgangspunkt også skifte fra én udbyder til en anden. Den pågældende overgår derved til en anden netstruktur og kan i dette andet net identificere sig med en anden brugeridentitet end i det tidligere net (i den udstrækning, der overhovedet skal angives en brugeridentitet). Det indebærer således et stort udredningsarbejde at fastlægge en målpersons nettrafik, når det skal sammenstykkes af trafikinformation fra mere end én internetudbyder og efter omstændighederne baseret på flere brugeridentiteter.

Hvis de involverede personer konsekvent kommunikerer over internettet ved brug af eksempelvis "anonyme" hotspots, vil det tilsvarende kunne være endog særdeles vanskeligt i forbindelse med en konkret efterforskning at fastlægge identiteten på de personer, som en given målperson kommunikerer med, og som det efter omstændigheder måtte stå klart er medskyldige i de forhold, som efterforskningen vedrører.

I forhold til sager om terrorisme og alvorlig organiseret kriminalitet har Politiets Efterretningstjeneste oplyst, at det ikke er muligt for efterretningstjenesten at give et nøjagtigt billede af, i hvilket omfang målpersoner anvender hotspots, internetcafeer eller lignende for at sløre deres kommunikation. Dette skal særligt ses i lyset af, at mulighederne for at skaffe sig adgang til en internetforbindelse er mangfoldige, og at afdækning af en målpersons anvendelse af offentligt tilgængelige internetforbindelser, som f.eks. et hotspot, derfor typisk kræver, at målpersonen bliver observeret i forbindelse med anvendelsen af internetforbindelsen.

Politiets Efterretningstjeneste kan imidlertid konstatere, at stort set alle efterretningstjenestens målpersoner udveksler kommunikation af relevans for efterretningstjenestens efterforskning via internettet. Samtidig er målpersonerne generelt meget sikkerhedsbevidste og træffer derfor typisk en række foranstaltninger for at skjule deres kommunikation. En metode hertil kan bl.a. være anvendelse af hotspots eller andre offentligt tilgængelige internetforbindelser, hvor der ikke stilles krav om valideret brugerregistrering.

Rigspolitiet har i tilknytning hertil oplyst, at målpersonerne i forbindelse med anden organiseret kriminalitet fortsat i første række anvender traditionel mobiltelefoni som deres primære kommunikationsform, og

at internetbaseret kommunikation (herunder via hotspots mv.) for de fleste kriminalitetsformer aktuelt spiller en mindre, men dog stigende rolle. Særligt i sager om børnepornografi ses en stigende anvendelse af uregistreret mobilt internet og hotspots i forbindelse med kommunikation og udveksling af filer. Et i nogen grad tilsvarende billede tegner sig for så vidt angår misbrug af betalingskort over internettet.

Det er Rigspolitiets overordnede vurdering, at den meget varierede adgang til internettet, som – hvis en given bruger ønsker det – i vid udstrækning kan opnås uden angivelse af valide identitetsoplysninger, udgør en stor efterforskningsmæssig udfordring, eksempelvis når en målpersons samlede kommunikation skal analyseres.

Såvel Politiets Efterretningstjeneste som Rigspolitiet vurderer på den baggrund, at en generel registrering af validerede identitetsoplysninger på brugere af offentligt tilgængelige internetforbindelser vil rumme betydelige efterforskningsmæssige fordele, særligt i sager om terrorisme, børnepornografi og visse andre former for organiseret kriminalitet.

7. Det politimæssige behov for udvidelse af kredsen af pligtsubjekter i henhold til logningsbekendtgørelsen

7.1. På baggrund af en politimæssig vurdering af behovet for at kunne tilvejebringe valide oplysninger om identiteten på brugere af internettet (jf. pkt. 6 ovenfor) har arbejdsgruppen drøftet, om et krav om registrering og validering af oplysninger om identiteten på brugere af internetadgang alene bør gælde for de udbydere, der i dag er omfattet af logningsbekendtgørelsen, eller om den også bør gælde for andre, der stiller internetadgang til rådighed for slutbrugere.

Det har i den forbindelse været arbejdsgruppens opfattelse, at selv om der indføres et krav om, at de udbydere, der er omfattet af den gældende logningsforpligtelse (de kommercielle udbydere), skal registrere og validere identitetsoplysninger på brugere af internettet, vil der fortsat være rig mulighed for, at personer, som ønsker at unddrage sig politiets efterforskning, kan kommunikere anonymt ved brug af eksempelvis trådløse net, der på ikke-kommercielt grundlag er stillet til rådighed for offentligheden, eller ved brug af computere med internetadgang på biblioteker mv.

Indførelse af et krav om brugerregistrering vil således ikke løse de efterforskningsmæssige problemer, som ifølge politiet er forbundet med den nugældende ordning, hvis kravet ikke udstrækkes til også at omfatte bl.a. biblioteker og kommunale hotspots, som i dag ikke er omfattet af logningsbekendtgørelsen, men som i meget vid udstrækning stiller internet til rådighed for offentligheden.

Hertil kommer, at en ordning med effektiv brugerregistrering på det kommercielle område – med de forbedrede efterforskningsmuligheder det vil indebære for politiet – ikke nødvendigvis vil stå i et rimeligt forhold til de omkostninger, det vil indebære for de kommercielle udbydere, hvis der ikke samtidig tilvejebringes tilsvarende løsninger i forhold til kommunikation, som sker via internetadgang, der stilles til rådighed af ikke-kommercielle parter.

Det er således arbejdsgruppens opfattelse, at en række praktiske og principielle betragtninger taler for at lade brugerregistreringen gælde for alle, der stiller internet til rådighed for en bredere offentlighed, uanset om dette sker på kommercielt eller ikke-kommercielt grundlag.

7.2. Arbejdsgruppen har i forlængelse heraf drøftet, om indførelse af en pligt til at registrere og validere identiteten på brugere af internettet ikke kun for de kommercielle udbydere, men for alle, der stiller internet til rådighed for en bredere kreds, i givet fald bør ledsages af en tilsvarende udvidelse af kredsen af pligtsubjekter i henhold til logningsbekendtgørelsen generelt. En sådan udvidelse vil betyde, at de oplysninger om internettrafik, som i dag skal logges af udbydere i telelovens forstand (jf. telelovens § 2), også vil skulle logges af andre, der på ikke-kommercielt grundlag stiller internetadgang til rådighed for slutbrugeren (og som derfor ikke er "udbydere" i telelovens forstand).

Der stilles i dag i meget vidt omfang internetadgang til rådighed på bl.a. biblioteker, uddannelsesinstitutioner og hospitaler, der som udgangspunkt ikke er omfattet af logningsforpligtelsen. De internetsessioner, der kan knyttes til den enkelte brugers aktiviteter på internettet, vil her som udgangspunkt ikke efter de gældende regler blive registreret og opbevaret.

Uddannelsesinstitutioner

Danmarks IT-center for uddannelse og forskning (UNI•C) har oplyst, at man ikke er i besiddelse af nærmere oplysninger om, i hvilket omfang der stilles internetadgang til rådighed for studerende, lærere mv. på uddannelsesinstitutionerne under Undervisningsministeriets område.

UNI•C skønner imidlertid, at alle uddannelsesinstitutioner som udgangspunkt har computere med internetadgang, som kan benyttes af elever mv., og at en væsentlig del af uddannelsesinstitutionerne tillige stiller trådløst internet til rådighed. UNI•C anbefaler i den forbindelse, at uddannelsesinstitutionerne sikrer, at det ikke er muligt at få adgang til internettet via trådløse net uden anvendelse af et personligt login. UNI•C anbefaler endvidere, at der oprettes en brugerdatabase med brugernavn og password på alle brugere, således at de indtastede oplysninger i forbindelse med loginproceduren kan valideres mod databaseoplysningerne.

I det omfang gæster (forældre mv.) skal have adgang til det trådløse net, anbefaler UNI•C, at det også sker via login, og at uddannelsesinstitutionen i den forbindelse registrerer gæstens navn og adresse ved f.eks. at lade den pågældende udfylde og underskrive en formular.

Der findes ikke nærmere opgørelser over, i hvilken udstrækning UNI•C's anbefalinger i dag følges.

Som eksempel på, hvordan adgangen til internettet i dag er indrettet på en større uddannelsesinstitution, kan det nævnes, at Handelshøjskolen i København (Copenhagen Business School – CBS), der ultimo 2010 havde ca. 17.000 studerende, stiller trådløst internettet til rådighed på hele skolens område. Adgangen til internettet forudsætter som udgangspunkt, at brugeren angiver sit CBS-brugernavn og sin CBS-adgangskode. Begge dele sendes til de studerende ved studiets påbegyndelse.

Gæster kan få tidsbegrænset adgang til det trådløse net via en CBS-studerende, som kan oprette et gæstelogin for den pågældende.

På CBS Bibliotek, der er et offentlig tilgængeligt bibliotek, findes en række stationære computere, hvorfra besøgende kan få adgang til internettet uden anvendelse af login eller lignende.

Hospitaler

I 2009 var der 27 offentlige sygehusenheder i Danmark. Danske Regioner har oplyst, at alle sygehusene tilbyder internetadgang til patienter og i et vist omfang også til pårørende.

En række hospitaler har udgivet informationsmateriale om internetadgang for patienter mv. Det fremgår eksempelvis af en vejledning, der er udgivet af Herlev Hospital, at patienter kan få trådløs adgang til internettet, hvis de pågældende medbringer deres egen bærbare pc. For at opnå adgang til det trådløse net på hospitalet skal patienten oplyse sit navn og CPR-nummer, hvorefter den pågældende bliver tildelt et bruger-id og en adgangskode, der gælder under indlæggelsen (dog normalt højst 7 dage).

Biblioteker

Ifølge Styrelsen for Bibliotek og Medier var der i 2009 499 folkebiblioteker, 38 statslige lovbiblioteker (herunder bl.a. Det Kongelige Bibliotek, Statsbiblioteket og en række universitetsbiblioteker) og 61 andre forskningsbiblioteker ved gymnasier, handelsskoler, landsbrugsskoler mv.

Samtlige biblioteker stiller i dag internet til rådighed for brugere i form af stationære computere med internetadgang og/eller trådløse net.

I foråret 2010 stillede 29 af de 32 lovbiblioteker (90,6 %) og 80 ud af landets 97 kommunale biblioteksvæsener (82,5 %) trådløs internetadgang til rådighed for besøgende.

I 2009 stillede folkebibliotekerne i alt 5.063 computere til rådighed for besøgende, hvoraf de 4.658 var opkoblet til internettet.

Som eksempel på administrationen af internetadgangen på et statsligt bibliotek kan det nævnes, at på Det Kongelige Bibliotek, der har publikumsafdelinger fire steder i København, kan alle besøgende få adgang til internettet via trådløst net eller via bibliotekets stationære computere. I begge tilfælde etableres adgangen til internettet uden anvendelse af login, og uden at brugeren på anden måde skal legitimere sig.

Når de forhold, der taler for indførelse af en brugerregistreringsordning, er de samme for kommercielle udbydere og for ikke-kommercielle parter, vil det tilsvarende gøre sig gældende for så vidt angår spørgsmålet om logning af oplysninger om teletrafik i øvrigt. Den efterforskningsmæssige værdi af en registreret brugeroplysning, vil således være meget begrænset, hvis der ikke samtidig er tilgængelige oplysninger om, hvem den pågældende har kommunikeret med, eller hvilke IP-adresser, der er knyttet til de hjemmesider mv., som den pågældende har besøgt.

Arbejdsgruppen finder på den baggrund, at en eventuel indførelse af en brugerregistreringsordning bør ledsages af, at logningsforpligtelsen efter logningsbekendtgørelsen udvides til også at omfatte ikke-kommercielle leverandører af internet.

8. Udenlandske erfaringer med brugerregistrering

IT- og Telestyrelsen har gennem det fælleseuropæiske samarbejde IRG-net søgt at indhente oplysninger om omfanget af de europæiske landes

erfaringer med visse aspekter af logning samt brugerregistrering[1]. I flertallet af de andre EU-lande fremgår det, at pligten til at registrere brugere er i overensstemmelse med logningsdirektivets udgangspunkt og derved i overensstemmelse med den gældende retstilstand i Danmark, idet logningen alene omfatter oplysninger, der allerede behandles eller genereres i udbydernes net.

Det fremgår således ikke af tilbagemeldingerne, at der i de pågældende lande skulle være erfaringer med registrering af brugere af hotspots mv.

9. Arbejdsgruppens overvejelser om en ændret afgrænsning af kredsen af logningsforpligtede

9.1. Kredsen af logningsforpligtede

9.1.1. Som det fremgår af afsnit 7 ovenfor, er det arbejdsgruppens opfattelse, at en eventuel indførelse af en brugerregistreringsordning i givet fald bør ledsages af et opgør med det hidtidige princip om, at logningsforpligtelsen påhviler *alle* kommercielle udbydere, *men ingen*, der på ikke-kommercielt grundlag stillet internet til rådighed for slutbrugere.

Det har i den forbindelse været arbejdsgruppens opfattelse, at den ganske omfattende logning af teleoplysninger, som finder sted i medfør af de gældende logningsregler, kun i begrænset omfang sikrer, at politiet i sager om alvorlig kriminalitet kan få adgang til relevante oplysninger om teletrafik, så længe der er almindelig adgang til at benytte internettet på steder og under forhold, som er undtaget fra logningsforpligtelsen.

Det politimæssige behov for at kunne få adgang til oplysninger om trafikdata og brugeridentiteter taler for, at også parter, der på ikke-kommercielt grundlag stiller internetadgang til rådighed for en bredere offentlighed, bør omfattes af logningsforpligtelsen.

9.1.2. Parter, der på ikke-kommercielt grundlag stiller internetadgang til rådighed for andre, vil overordnet kunne inddeles i to grupper.

---

[1] IT- og Telestyrelsen har modtaget oplysninger fra henholdsvis Tyskland, Frankrig, Finland, Østrig, Irland, Kroatien, Storbritannien, Polen, Schweiz, Ungarn, Slovakiet og Portugal.

Den ene gruppe vil være kendetegnet ved, at anvendelsen af de pågældende net eller tjenester er forbeholdt en bestemt personkreds, som (uafhængigt af deres ønske om at benytte internettet) kan afgrænses på forhånd, og hvis identitet er kendt af udbyderen (f.eks. studerende på en uddannelsesinstitution eller medarbejdere på en arbejdsplads). Den anden gruppe vil i den sammenhæng være kendetegnet ved, at brugerkredsen ikke på forhånd kan afgrænses, idet adgangen i princippet er til rådighed for alle (f.eks. brugere af biblioteker eller hotspots).

En afvejning af hensynet til det politimæssige behov for at kunne få adgang til oplysninger om teletrafik fra de enkelte brugere over for hensynet til ikke at pålægge parterne unødvendige byrder, tilsiger, at logningsforpligtelsen efter en eventuel ændring af ordningen alene kommer til at omfatte parter, der stiller internet til rådighed for en *ikke på forhånd* afgrænset kreds af personer.

Med en sådan afgrænsning vil eksempelvis arbejdspladser, uddannelsesinstitutioner og hospitaler, hvis it-systemer er indrettet, så alene medarbejdere, studerende og patienter har adgang til internettet, blive holdt uden for logningsforpligtelsen, mens eksempelvis folkebiblioteker, internetcafeer, offentlige transportmidler, kommunale hotspots mv. vil være omfattet af logningsforpligtelsen.

En sådan afgrænsning af kredsen af logningsforpligtede vil efter Rigspolitiets og Politiets Efterretningstjenestes opfattelse give politiet et tilstrækkeligt sikkert og i forhold til i dag mærkbart forbedret grundlag for efterforskning på baggrund af internetkommunikation.

9.1.3. Det er i forlængelse heraf også den politifaglige vurdering, at det politimæssige behov er det samme i forhold til kommercielle udbydere som i forhold til ikke-kommercielle.

Det er derfor arbejdsgruppens opfattelse, at en udvidelse af kredsen af logningsforpligtede i forhold til ikke-kommercielle aktører, bør ledsages af en indskrænkning i kredsen af logningsforpligtede kommercielle udbydere, således at der bliver parallelitet imellem de to grupper. Derved vil det ikke i forhold til logningsforpligtelsen være afgørende, om eksempelvis et hospital drives i privat eller offentligt regi, men alene om den internetadgang, som i givet fald stilles til rådighed på det pågældende hospital, kan siges at være alment tilgængelig eller er forholdt en på forhånd afgrænset personkreds.

Dette vil i praksis betyde, at en række kommercielle aktører, som i dag er omfattet af logningsforpligtelsen, ikke vil være det i fremtiden. Således vil eksempelvis privathospitaler, private uddannelsesinstitutioner, hoteller, fitnesscentre mv. have mulighed for at indrette sig på en måde, der indebærer, at de ikke vil være forpligtet til at foretage logning.

9.1.4. I forhold til de parter, der ved den skitserede afgrænsning ikke omfattes af logningsforpligtelsen, bemærkes, at oplysninger om den samlede trafik ind og ud af eksempelvis en uddannelsesinstitution vil blive logget af den udbyder, som leverer internet til institutionen. Politiet vil således i forbindelse med en konkret efterforskning kunne konstatere, at den pågældende kommunikation hidrører fra institutionen, og vil således kunne koncentrere efterforskningen mod kredsen af studerende eller medarbejdere mv. ved den pågældende institution.

Er der tale om en mindre institution, vil denne oplysning typisk i sig selv være tilstrækkelig til, at politiet ved sædvanlige efterforskningsskridt vil kunne fastlægge identiteten på den pågældende bruger.

Er der tale om en større institution, vil institutionen i øvrigt normalt selv foretage en registrering (hvis ikke af teletrafikken så i hvert fald) af oplysninger om, hvilke brugere der har været logget på nettet på et givent tidspunkt og på hvilke maskiner.

9.1.5. I forhold til oplysninger om internettrafik fører disse betragtninger efter arbejdsgruppens opfattelse frem til, at kredsen af logningsforpligtede (efter en eventuel ændring af de gældende regler) bør omfatte alle, der stiller internet til rådighed for en ikke på forhånd afgrænset kreds af brugere.

For at falde uden for kredsen af logningsforpligtede, må den, der stiller internetadgang til rådighed, således forbeholde internetadgangen for en på forhånd afgrænset kreds af personer.

I udtrykket en "på forhånd afgrænset kreds af personer" ligger i denne sammenhæng et krav om,

- at det, der knytter personkredsen sammen, skal være forhold, der ikke vedrører de pågældendes internetrelaterede aktiviteter,
- at den, der stiller internettet til rådighed, har et samlet overblik over, hvem personkredsen består af,

- at den, der stiller internettet til rådighed, har betydelig sikkerhed for identiteten på de personer, der indgår i kredsen,
- at kredsen ikke er for bred til, at den vil udgøre et brugbart udgangspunkt for en politimæssig efterforskning, og
- at internetadgangen er effektivt skærmet, således at den alene kan anvendes af den afgrænsede personkreds.

9.2. Forholdet til logningsdirektivet

Som nævnt ovenfor under pkt. 4.4 omhandler logningsdirektivet "udbydere af offentligt tilgængelige elektroniske kommunikationstjenester eller af et offentligt kommunikationsnet", men direktivet indeholder ikke en nærmere definition af begrebet udbyder. Det er således overladt til den enkelte medlemsstat at foretage den nærmere regulering heraf. I den forbindelse har medlemsstaterne mulighed for at fastsætte regler, der er mere vidtgående end direktivet.

Arbejdsgruppen har i lyset af direktivteksten fokuseret på at sikre en afgrænsning af "udbyderbegrebet", som omfatter alle "offentligt tilgængelige elektroniske kommunikationstjenester" og alle "offentlige kommunikationsnet".

Endvidere har arbejdsgruppen overvejet, om det i forhold til logningsdirektivet vil kunne udgøre et problem, at arbejdsgruppens afgrænsning af udbyderbegrebet adskiller sig fra det udbyderbegreb, der er gennemført i dansk ret som led i implementeringen af bl.a. EU-direktiverne om fælles rammebestemmelser for elektroniske kommunikationsnet og -tjenester (direktiv 2002/21EF) og om behandling af personoplysninger og beskyttelse af privatlivets fred i den elektroniske kommunikationssektor (direktiv 2002/58/EF).

Det er imidlertid arbejdsgruppens vurdering, at der ikke med de nævnte direktiver er forudsat en ensartethed i anvendelsen af udbyderbegrebet, ligesom der efter arbejdsgruppens opfattelse ikke er en sådan sammenhæng mellem logningsdirektivet og de øvrige EU-regler, at en sådan ensartethed er fornøden.

Det er således arbejdsgruppens vurdering, at den ovenfor skitserede fastlæggelse af kredsen af pligtsubjekter, vil omfatte alle sådanne offentligt tilgængelige services og således være i overensstemmelse med direktivet.

Med udgangspunkt i de ovenfor i punkt 9.1.5 anførte kriterier for hvad der må anses for "en på forhånd afgrænset kreds af personer" vil de kommunikationstjenester og kommunikationsnet, der efter den skitserede model holdes uden for logningsforpligtelsen, ikke med rimelighed kunne opfattes som "offentlige".

9.3. Nærmere om de enkelte kriterier efter den skitserede model

9.3.1. Da der er en række retsvirkninger forbundet med at falde henholdsvis inden for og uden for kredsen af logningsforpligtede, vil der efter en eventuel ændring af kredsen af logningsforpligtede – i lighed med efter den gældende ordning – opstå situationer, hvor der vil skulle tages stilling til, om konkrete parter, der stiller internet til rådighed for en bredere kreds, er omfattet af logningsforpligtelsen eller ikke, og hvor svaret umiddelbart vil kunne forekomme tvivlsomt.

Arbejdsgruppen vurderer, at langt de fleste parter, der stiller internet til rådighed for en bredere kreds, uden videre vil kunne placeres i enten den ene eller den anden gruppe, og at afgrænsningsproblemerne i praksis ikke vil blive større end efter den eksisterende ordning. Arbejdsgruppen har imidlertid overvejet en række grænsetilfælde og har på den baggrund fundet det hensigtsmæssigt i det følgende at foretage en nærmere gennemgang af hvert af de i afsnit 9.1.5. anførte kriterier.

9.3.2. I forudsætningen om, at personkredsen skal være afgrænset *på "forhånd"*, ligger et krav om, at *det, der knytter personkredsen sammen, skal være forhold, der ikke vedrører de pågældende personers internetrelaterede aktiviteter.*

Det vil dels indebære, at personkredsen ikke kan fastlægges som de, der på et givent tidspunkt opholdt sig på eksempelvis en given internetcafe, men det indebærer endvidere, at personkredsen skal kunne afgrænses på grundlag af noget andet end et fælles ønske om at etablere internetadgang. Dette vil eksempelvis betyde, at formodningen vil være imod, at man kan falde uden for logningsforpligtelsen ved at henvise til, at personkredsen er begrænset til medlemmer af en given forening eller lignende, hvis foreningen har som en central del af sit formål at opnå adgang til internettet.

9.3.3. Kravet om, at kredsen skal være *"afgrænset"*, indebærer bl.a., at den, der stiller internetadgangen til rådighed, skal have et *samlet overblik*

over, hvem personkredsen består af og – i lyset af formålet med logningsreglerne – det seneste år har bestået af (eksempelvis ved at være i besiddelse af et medlemskartotek og kunne føre dette mindst et år tilbage). Det vil således ikke være tilstrækkeligt til, at man efter den foreslåede model kan falde uden for logningsforpligtelsen, at man kan henvise til, at adgangen i praksis er begrænset til personer, der eksempelvis på et givet tidspunkt er medlemmer af eller tilknyttet en given forening eller organisation, hvis den, der stiller internettet til rådighed, ikke er i besiddelse af oplysninger om, hvem der konkret hører og det seneste år har hørt til den afgrænsede personkreds.

Dette vil bl.a. betyde, at de enkelte deltagere i eksempelvis en sammenslutning af private indehavere af trådløse net, som stiller deres respektive net til rådighed for hinanden, ikke vil kunne falde uden for logningsforpligtelsen, hvis sammenslutningens "deltagerliste" administreres af en enkelt af deltagerne eller af en tredjepart. De enkelte netindehavere vil i en sådan konstruktion stille nettet til rådighed for en kreds af brugere, som de ikke selv kender identiteten på, og som derfor ikke for den enkelte netindehaver er afgrænset. Hvis det at dele hinandens net i øvrigt er det centrale element i en sammenslutning af denne art, vil det tillige være tvivlsomt, om kredsen kan siges at kunne fastlægges på "forhånd", jf. pkt. 9.3.2 ovenfor.

Endvidere vil det omtalte kriterium indebære, at det vil være en forudsætning for, at eksempelvis boligforeninger (på samme måde som uddannelsesinstitutioner, hoteller mv.) vil kunne holdes uden for logningsforpligtelsen, at adgangen til at benytte nettet er forbeholdt den relevante kreds af personer (foreningens beboere).

Det vil i den forbindelse være en forudsætning, at boligforeningen indskærper over for beboerne, at alene personer med bopæl på stedet må anvende nettet, og i den udstrækning der anvendes trådløse løsninger, at disse forsynes med adgangskode mv. Denne begrænsning svarer til den, der gælder for uddannelsesinstitutioner, arbejdspladser mv. og uden hvilken, den, der stiller internet til rådighed (eksempelvis boligforeninger), ikke vil have et samlet overblik over, hvem kredsen af mulige brugere består af. Konsekvensen heraf vil være, at eksempelvis boligforeningen (på samme måde som andre, der udbyder internet til private husstande) vil skulle foretage logning i overensstemmelse med logningsbekendtgørelsen.

Spørgsmålet om, hvorvidt den enkelte husstand vil blive pålagt restriktioner i sin mulighed for at lade eksempelvis gæster benytte sit net, vil således afhænge af, om den udbyder, der stiller nettet til rådighed for husstanden, foretager logning – uanset om udbyderen er en boligforening eller eksempelvis et teleselskab.

9.3.4 I forlængelse heraf indebærer forudsætningen om, at internetadgangen skal være forbeholdt en på forhånd fastlagt kreds af personer i form af eksempelvis patienter, studerende, medarbejdere eller medlemmer, endvidere, at den der stiller internettet til rådighed skal have *betydelig sikkerhed for identiteten på de personer, der indgår i kredsen.*

Det vil være vanskeligt at udstikke meget præcise retningslinjer for, hvad der i forhold til eksempelvis mindre foreninger mv. vil skulle til, for at kendskabet til identiteten på de enkelte personer, der indgår i personkredsen, kan siges at være tilstrækkeligt sikkert. Men det er oplagt, at en institution eller forening, til hvilken man kan blive tilknyttet, ved uden nogen forudgående tilknytning til institutionen at gå ind fra gaden og skrive sit navn på en liste, ikke vil leve op til kravet om, at personkredsen skal være afgrænset på forhånd.

For så vidt angår eksempelvis hoteller, hvor gæsternes tilknytning er ganske kortvarig, og hvor hotellets personale ikke nødvendigvis har anden kontakt til gæsterne end den, der finder sted i forbindelse med ind- og udskrivning, må der stilles ganske betydelige krav til sikkerheden for identiteten på de pågældende personer (ligesom det i øvrigt vil være nødvendigt at indskærpe over for gæsterne, at internetadgangen er personlig og ikke må stilles til andres rådighed).

Som det fremgår af afsnit 9.3.3 ovenfor, må det endvidere forudsættes, at det enkelte hotel er i stand til at føre sit kendskab til gæsterne et år tilbage.

Omvendt vil det for eksempelvis små foreninger, hvor medlemskabet i praksis er forbundet med personligt kendskab, ikke nødvendigvis være en forudsætning, at den tilknyttede personkreds i forbindelse med indskrivning eller lignende har fremvist særlig legitimation, eller at de oplyste identitetsoplysninger i øvrigt har været genstand for en eller anden form for kontrol. Det vil imidlertid også i forhold til sådanne mindre institutioner, foreninger mv. være en forudsætning for ikke at blive omfattet af

logningsforpligtelsen, at internetadgangen på effektiv vis er afskåret for andre end den tilknyttede personkreds.

9.3.5. Endelig vil kravet om, at personkredsen skal være afgrænset, også skulle ses i lyset af den politimæssige interesse, der vil skulle varetages ved indførelse af logningsregler efter de her skitserede principper. Dette vil betyde, at kredsen ikke kan anses for afgrænset, hvis den er så bred, at den ikke vil udgøre noget brugbart udgangspunkt for en politimæssig efterforskning.

Denne grænse kan efter arbejdsgruppens opfattelse ikke fastsættes til et eksakt antal brugere, idet vurderingen af, om antallet i sig selv gør, at kredsen er for bred til, at den kan siges at udgøre en politifagligt relevant afgrænsning, også vil bero på graden af sammenhæng i personkredsen, hvor stabil denne kreds må antages at være, og hvilken grad af kontrol, den der stiller internettet til rådighed for brugerne, må antages at have med, at alene berettigede brugere anvender nettet.

Det er imidlertid arbejdsgruppens opfattelse, at der alene vil være anledning til at overveje, om personkredsen er for bred, hvis der er tale om en kreds på mere end 1.000 personer.

Er den pågældende brugerkreds større end tusinde, vil det skulle vurderes på baggrund af de ovenfor nævnte kriterier, om brugerkredsen konkret kan anses for afgrænset tilstrækkeligt til, at der vil være et anvendeligt politifagligt udgangspunkt for en videre efterforskning.

Det er i den forbindelse umiddelbart arbejdsgruppens opfattelse, at hvis der er tale om en institution, hvor der må antages at være et vist personligt kendskab internt i kredsen, hvor personkredsen ikke generelt ændres fra dag til dag, hvor enhver ikke af egen drift kan tilknytte sig, og hvor der føres en vis egenkontrol med anvendelsen af internettet, vil antallet af tilknyttede personer kunne være *betydeligt højere* end 1.000.

Arbejdsgruppen har i den forbindelse fundet, at eksempelvis kredsen af medarbejdere i landets største kommuner eller kredsen af studerende og medarbejdere ved landets største uddannelsesinstitutioner (som i begge tilfælde vil kunne udgøre op til ca. 40.000 personer) ikke i sig selv – trods det store antal personer – er så bred, at det udelukker, at kommunen eller uddannelsesinstitutionen kan holdes uden for logningsforpligtelsen (hvis betingelserne herfor i øvrigt er opfyldt).

Omvendt er det umiddelbart arbejdsgruppens opfattelse, at kredsen af medarbejdere i eksempelvis en af landets største lufthavne eller et af de største indkøbscentre (der vil udgøre betydeligt færre end 40.000) som udgangspunkt ikke vil være tilstrækkeligt afgrænset, idet der ikke vil være en tilstrækkelig sammenhæng i den pågældende personkreds, da medarbejderne typisk vil være ansat i en lang række selvstændige firmaer med individuelle opgaver, ansættelsesvilkår og ansættelsesprocedurer mv.

Samtidig er det vurderingen, at hvis eksempelvis en af de største danske banker (som tæller deres privatkunder i adskillige hundrede tusinder) stiller trådløst net til rådighed for deres kunder i samtlige filialer, vil banken skulle foretage logning. Uanset hvilke betingelser og sikkerhedsprocedurer, der måtte knyttes til kundeforholdet, vil en så omfattende personkreds ud fra en politifaglig vurdering ikke give noget reelt udgangspunkt for en videre efterforskning, og personkredsen kan således ikke anses som på forhånd afgrænset.

9.3.6. Endelig indebærer kravet om, at kredsen skal være afgrænset tillige, at *internetadgangen er effektivt afskærmet*, så alene den afgrænsede personkreds ad denne vej kan få adgang til internettet.

Har eksempelvis en arbejdsplads eller en uddannelsesinstitution ikke sikret sit net med individuelle brugernavne og koder til medarbejdere eller studerende (og ledsage disse med en angivelse af, at adgangen er personlig og ikke må udlånes til andre), vil adgangen til internettet ikke i praksis være begrænset til de pågældende personer, og arbejdspladsen eller uddannelsesinstitutionen vil dermed som udgangspunkt blive omfattet af logningsforpligtelsen.

På tilsvarende måde vil institutioner, som tillader, at gæster ved brug af et gæste-login får adgang til internettet via institutionens net, ikke leve op til kravet om en på forhånd afgrænset brugerkreds, og institutionen vil derfor blive omfattet af logningsforpligtelsen. Institutioner, som ønsker at levere internetadgang til deres gæster, vil imidlertid ved at stille et separat net til rådighed for gæster kunne nøjes med at lade dette separate net omfatte af logningsreglerne og de hertil knyttede regler om brugerregistrering.

10. Arbejdsgruppens overvejelser om indretning af en ordning med registrering af validerede brugeroplysninger

Det følger i dag af logningsbekendtgørelsens § 1, at udbydere af elektroniske kommunikationsnet eller -tjenester til slutbrugere skal foretage registrering og opbevaring af oplysninger om teletrafik, der genereres eller behandles i udbyderens net, således at disse oplysninger vil kunne anvendes som led i efterforskning og retsforfølgning af strafbare forhold.

Logningsforpligtelsen er således begrænset til oplysninger, der genereres eller behandles i udbyderens net, og logningsbekendtgørelsen indeholder i dag ingen krav om, hvilke oplysninger der skal genereres eller behandles.

Som anført ovenfor vil der i en række tilfælde ikke være anledning for udbyderne til at generere eller behandle oplysninger om brugeridentitet, hvorfor sådanne oplysninger i praksis meget ofte heller ikke registreres.

En effektiv ordning for registrering af brugere af internetnetadgang vil derfor forudsætte, at der gøres op med det nævnte princip om, at logningsforpligtelsen alene omfatter oplysninger, der uafhængigt af logningsreglerne genereres og behandles i udbyderens net.

Der vil således skulle indføres en forpligtelse for udbydere til at tilvejebringe, registrere og opbevare oplysninger om brugernes identitet også i situationer, hvor disse oplysninger ikke i dag behandles i udbyderens net (typisk fordi oplysningerne er uden betydning for levering af udbyderens tjenester).

Endvidere vil der skulle stilles krav om, at de tilvejebragte identitetsoplysninger valideres.

Som det fremgår af pkt. 6 ovenfor, er det Rigspolitiets og Politiets Efterretningstjenestes opfattelse, at en valideret registrering af brugere af internetforbindelser vil rumme betydelige efterforskningsmæssige fordele, idet bl.a. Politiets Efterretningstjenestes målpersoner i vid udstrækning søger at skjule deres kommunikation bl.a. ved at anvende offentligt tilgængelige internetforbindelser, hvor der ikke foretages registrering og validering af identitetsoplysninger.

For at kunne imødekomme det politimæssige behov for at sikre identiteten på personer, der kommunikerer via internettet, vil indførelsen af en brugerregistreringsordning – både af hensyn til politiets efterforskning og dermed indirekte af hensyn til proportionaliteten i forhold til de omkostninger, der for udbyderne vil være forbundet med registreringen – skulle indrettes på en sådan måde, at den i videst muligt omfang afskærer muligheden for at bruge falske identiteter.

Det bør således indgå som en afgørende forudsætning i en eventuel brugerregistreringsordning, at brugeren ikke får adgang til internettet, før oplysningerne om den pågældendes identitet er valideret og registreret hos udbyderen. Identifikationen bør i den forbindelse være entydig og bygge på oplysninger, der er egnede til umiddelbart at blive valideret. Tilsvarende må de oplysninger, der danner grundlag for valideringen, være af en sådan karakter, at de yder den fornødne beskyttelse mod misbrug.

Foruden at sikre den efterforskningsmæssige værdi af identitetsoplysningerne vil en forudgående eller samtidig validering af oplysningerne også medvirke til at minimere risikoen for, at uskyldige personer bliver gjort til genstand for en politimæssig efterforskning, fordi oplysninger om den pågældendes identitet er blevet misbrugt.

Det er i forlængelse heraf arbejdsgruppens opfattelse, at en valideringsproces for at være anvendelig må skulle kunne gennemføres umiddelbart og uden at indebære en nævneværdig forsinkelse af adgangen til internettet. Det vil således normalt være afgørende for anvendelsen af eksempelvis et hotspot, at der kan opnås adgang til internettet relativt hurtigt.

Det bemærkes, at de identitetsoplysninger som valideres og registreres i udbyderens net, efter arbejdsgruppens opfattelse ikke nødvendigvis behøver at bestå af navn og adresse. Efter omstændighederne vil udbyderne i stedet kunne registrere et oplyst (og valideret) CPR-nummer, et betalingskortnummer, et telefonnummer eller andre oplysninger, så længe der er den fornødne sikkerhed for, at de registrerede oplysninger kan føres tilbage til den faktiske bruger med samme sikkerhed som registrering af et navn og en adresse.

De oplysninger, som er blevet indhentet til brug for arbejdsgruppens arbejde, viser, at der allerede i dag – uanset at der ikke i lovgivningen stilles krav herom – i en lang række sammenhænge foretages registrering og

validering af brugeridentiteter i forbindelse med adgang til internettet. Dette gælder ikke kun i forbindelse med internetadgang, for hvilken der skal erlægges betaling, men også for internetadgang der stilles gratis til rådighed.

Arbejdsgruppen har således på baggrund bl.a. af oplysninger om eksisterende procedurer drøftet de modeller for brugerregistrering, som er beskrevet i det følgende.

10.1. Validering baseret på CPR-nummer

Validering af afgivne identitetsoplysninger sker i dag i en række sammenhænge på baggrund af opslag i Det Centrale Personregister. Det sker eksempelvis ofte i forbindelse med tegning af faste abonnementer på telefoni eller internet.

I forbindelse med adgang til internettet fra offentligt tilgængelige trådløse eller kablede forbindelser vil en CPR-baseret validering kunne foretages ved, at brugeren ved opstart af browseren på en computer anmodes om at indtaste navn, adresse og CPR-nummer, hvorefter teleudbyderen via Det Centrale Personregister sammenholder personnummeret med de øvrige personoplysninger. Hvis der er overensstemmelse mellem de indtastede oplysninger og oplysningerne i Det Centrale Personregister, etableres der automatisk adgang til internettet.

På Odense Universitetshospital er der trådløs adgang til internettet for patienter og pårørende. Når brugeren starter sin browser for at gå på internettet, bliver den pågældende automatisk dirigeret videre til en login-side, hvor navn, postnummer på hjemadresse og CPR-nummer skal oplyses. Oplysningerne bliver herefter valideret mod Det Centrale Personregister. Hvis der er overensstemmelse mellem de indtastede oplysninger og oplysningerne i Det Centrale Personregister, etableres der automatisk adgang til internettet.

Det skal imidlertid bemærkes, at Indenrigs- og Sundhedsministeriets CPR-kontor efter en henvendelse fra Datatilsynet for nyligt har ændret vilkårene for opslag i CPR ved anvendelse af digitale selvbetjeningsløsninger på internettet.

Baggrunden herfor er, at en række af CPR's kunder har indrettet deres selvbetjeningsløsninger således, at brugeren i forbindelse med oprettelse af et kundeforhold, medlemskab eller lignende skal indtaste navn og CPR-nummer. Såfremt en validering mod CPR bekræfter, at der er sam-

menhæng mellem de indtastede data, vil brugeren få adgang til næste trin i processen. I modsat fald anmodes den pågældende om at indtaste navn og personnummer på ny.

Datatilsynet har fundet, at denne fremgangsmåde udgør en potentiel sikkerhedsrisiko, og har i den forbindelse henvist til, at den dataansvarlige efter persondatalovens § 41, stk. 3, skal træffe de fornødne tekniske og organisatoriske sikkerhedsforanstaltninger mod, at oplysninger bl.a. kommer til uvedkommendes kendskab eller misbruges.

Selv om flere digitale selvbetjeningsløsninger alene stiller et begrænset antal forsøg til rådighed for validering, har Datatilsynet tilkendegivet, at med et stigende antal digitale selvbetjeningsløsninger vil risikoen for misbrug af adgangen til at slå data op i CPR blive uacceptabelt høj. Det bemærkes i den forbindelse, at der til en given fødselsdato og et givent køn alene findes 270 valide CPR-numre.

CPR-kontoret har på baggrund af Datatilsynets bemærkninger anført følgende i kontorets standardvilkår:

"Anvendes adgangen til CPR i forbindelse med elektronisk selvbetjening, skal kunden sikre, at uvedkommende ikke herigennem kan få adgang til CPR-oplysninger eller få bekræftet eller afkræftet en eventuel sammenhæng mellem et navn og et CPR-nummer. Tilbagemeldinger på indtastede data skal således være af en karakter, der ikke afslører resultatet af en validering mod CPR."

Den enkelte kunde afgør dog selv, hvorledes man i givet fald vil indrette sin selvbetjeningsløsning, så løsningen overholder CPR-kontorets standardvilkår og persondatalovens § 41, stk. 3.

Det er imidlertid arbejdsgruppens opfattelse, at man vanskeligt i forbindelse med en validering, der foretages med henblik på umiddelbart at opnå adgang til internettet, vil kunne indrette en CPR-baseret model, der vil kunne leve op til de nævnte standardvilkår.

Selv hvis en model baseret på validering ved brug af CPR-nummer kunne indrettes i overensstemmelse med de anførte retningslinjer, ville det efter arbejdsgruppens opfattelse være en ulempe ved modellen, at det i praksis er vanskeligt at skride effektivt ind over for misbrug af CPR-numre.

Kommer en tredjemand således uberettiget i besiddelse af en andens CPR-nummer og anvender det i forbindelse med brugeregistrering, vil det foruden at svække politiets mulighed for effektivt at efterforske på baggrund af den pågældende kommunikation også kunne indebære en betydelig gene for privatpersoner, der måske i længere tid må affinde sig med, at deres identitetsoplysninger bliver kædet sammen med eventuelle kriminelle forhold, uden at de pågældende i realiteten kan gøre noget for at hindre det.

I øvrigt bemærkes, at modellen i sagens natur alene kan anvendes over for personer, der har et dansk CPR-nummer.

10.2. Identifikation ved anvendelse af et telefonnummer (SMS-modellen)

I en række forskellige sammenhænge afsendes koder til elektroniske tjenester via SMS som en del af en valideringsproces. Dette gælder bl.a. i forbindelse med bekræftelse af større transaktioner i visse netbanker eller i forbindelse med, at en bruger af en elektronisk tjeneste har glemt eksempelvis en adgangskode.

I disse sammenhænge er anvendelsen af SMS imidlertid baseret på telefonnumre, som brugeren på et tidligere tidspunkt selv har oplyst, og som således ikke i sig selv gøres til genstand for validering.

En SMS-model i forbindelse med, at der åbnes for visse internetbaserede betalingstjenester, anvendes endvidere ikke for at validere identiteten på brugeren, men for via telefonregningen at opkræve betaling for tjenesten, eksempelvis internetadgang.

TDC har opsat hotspots en række steder i landet, som personer med et dansk SIM-kort kan købe adgang til.

Betalingen foregår ved, at den person, der ønsker at købe adgang til internettet, sender en SMS med et nærmere angivet indhold til nummeret 1230, hvorefter den pågældende modtager en SMS med brugernavn og adgangskode til TDCs hotspots. Der bliver i den forbindelse trukket et beløb fra det abonnement, der er knyttet til afsendernummeret. Det forudbetalte beløb modsvares af et nærmere angivet antal timer, hvor internetadgangen kan benyttes.

I den udstrækning et angivet telefonnummer er baseret på en abonnementsaftale, vil telefonnummeret imidlertid i realiteten være forbundet

med identitetsoplysninger, som er blevet valideret i forbindelse med abonnementsaftalen. Det vil således i en sådan situation være muligt på baggrund af oplysninger om telefonnummeret at tilvejebringe valide oplysninger om identiteten på indehaveren af det pågældende nummer.

En oplagt hindring for i dag at anvende en registrerings og valideringsmodel baseret på udveksling af SMS'er er eksistensen af uregistrerede taletidskort.

Commute Media (tidligere Gratis Danmark) har indgået aftale med Movia, Arriva og DSB om levering af trådløst internet i S-tog og på en række buslinjer.

Commute Media har over for arbejdsgruppen tilkendegivet, at man i forbindelse med etableringen af det trådløse internet i de nævnte offentlige transportmidler overvejede forskellige modeller, der kunne tilvejebringe oplysninger om den faktiske brugers identitet. Gratis Danmark fandt på daværende tidspunkt, at en løsning baseret på identifikationen af brugeren via anvendelse af et telefonnummer (SMS-model) umiddelbart ville udgøre det mest sikre og smidige grundlag for brugeridentifikation. På grund af udbredelsen af uregistrerede taletidskort valgte man imidlertid en anden løsning, der er baseret på brugervalidering via en angivet e-mail-adresse.

I den udstrækning der tilvejebringes en effektiv model for registrering af brugere af taletidskort, vil SMS-modellen imidlertid efter arbejdsgruppens vurdering kunne udgøre en enkel og effektiv metode til registrering af valide identitetsoplysninger.

Modellen – som i sagens natur forudsætter, at brugeren er i besiddelse af en mobiltelefon – vil kunne indrettes således, at brugeren ved opstart af browseren anmodes om at indtaste sit mobiltelefonnummer, hvorefter der sendes en adgangskode til det angivne telefonnummer. Brugeren kan herefter indtaste adgangskoden på computeren mv., hvorefter der etableres adgang til internettet.

Udbyderen vil i den forbindelse skulle registrere og opbevare oplysningen om det angivne telefonnummer, men ikke i øvrigt tage skridt i retning af at afdække bagvedliggende identitetsoplysninger.

Som nævnt vil modellen forudsætte, at der tilvejebringes en effektiv model for registrering af brugere af taletidskort. Det må endvidere være en forudsætning for, at modellen yder den tilstrækkelige sikkerhed for validiteten af oplysningerne, at der alene kan afsendes SMS'er til danske telefonnumre. Det vil således ikke være realistisk at tro, at man inden for

en overskuelig årrække vil have gjort op med anonyme taletidskort i alle dele af verden, hvorfor der ikke nødvendigvis vil være valide identitetsoplysninger knyttet til et udenlandsk telefonnummer.

For så vidt angår registrering af brugere af taletidskort henvises til arbejdsgruppens notat af 2. juli 2010.

10.3. Validering på baggrund af betalingskortoplysninger (betalingskortmodellen)

En validering på baggrund af betalingskortoplysninger vil i sin opbygning kunne svare til CPR-modellen, jf. pkt.10.1.

Brugeren anmodes om at indtaste sit kortnummer samt udløbsdato og kontrolnummer. På principielt samme måde som det sker i forbindelse med et almindeligt køb over internettet, bliver det på baggrund af de angivne oplysninger via Nets (tidligere PBS) eller anden international virksomhed, der håndterer betalinger med internationale betalingskort, undersøgt, om det pågældende kortnummer er gyldigt, og om kortet eventuelt er spærret.

Bekræftes kortets gyldighed, og er det ikke spærret, vil udbyderen herefter normalt i kortnummeret have en oplysning, som kan føres tilbage til en fysisk person.

Sealink Technology ApS leverer kablet og trådløst internet til bl.a. en række hoteller og havne. Internetadgangen for den enkelte bruger kan bl.a. etableres via betalingskort. Brugeren betaler forud for et antal timers internetadgang, og der indtastes som led heri de sædvanlige betalingskortoplysninger i form af kortnummer, udløbsdato og kontrolcifre. Efter PBS-valideringen modtager Sealink en e-mail fra PBS med et nummer for den pågældende transak-tion. Transaktionsnummeret opbevares af Sealink (sammen med den tildelte IP-adresse og data for internetsessionen), og oplysningerne herom kan efterfølgende anvendes til at identificere kortindehaveren, f.eks. i forbindelse med en strafferetlig efterforskning.

Nets har over for arbejdsgruppen oplyst, at en sådan forespørgsel vedrørende et betalingskorts gyldighed vil kunne gennemføres, uden at forespørgslen er forbundet med et træk på kundens betalingskort.

Arbejdsgruppen har i forbindelse med overvejelserne om anvendelse af betalingskortmodellen konstateret, at det visse steder i udlandet i dag er muligt at købe forudbetalte betalingskort gennem bl.a. Visa og Master-

Card. Kortene, der typisk bruges som gavekort, kan udstedes på et fastsat engangsbeløb, således at kortet kasseres, når beløbet er brugt. For sådanne kort sker der ingen registrering af identiteten på den, der opretter kortet. Et forudbetalt Visa eller MasterCard, der er udstedt i udlandet, vil også kunne anvendes til køb i danske butikker, der accepterer henholdsvis Visa og MasterCard. Det er i den forbindelse endvidere Nets vurdering, at forudbetalte kort i løbet af nogle år også vil kunne udstedes i Danmark.

Forudbetalte kort indeholder ligesom almindelige betalingskort et kortnummer på op til 16 cifre, en udløbsdato og tre kontrolcifre. Kortene adskiller sig således ikke umiddelbart fra andre typer af betalingskort.

I forbindelse med en almindelig forespørgsel vedrørende gyldigheden af et angivet kortnummer vil man ifølge Nets ikke modtage underretning om, at der tale om et forudbetalt uregistreret betalingskort.

På samme måde som for SMS-modellen vil validering på baggrund af et betalingskortnummer således ikke yde den tilstrækkelige sikkerhed, hvis det er muligt, at det angivne kortnummer dækker over et forudbetalt uregistreret kort.

Anvendelsen af en betalingskortmodel vil således forudsætte, at udbyderen sikrer sig, at adgangen til internettet alene åbnes, hvis det opgivne betalingskort foruden at være gyldigt hverken er spærret eller forudbetalt.

En sådan sikkerhed vil efter det for arbejdsgruppen oplyste kunne opnås, enten ved at der sendes en udvidet forespørgsel til Nets, som indeholder en specifik forespørgsel om, hvorvidt kortet er forudbetalt, eller ved at udbyderen selv kontrollerer kortselskabernes BIN-tabeller og indretter den software, som anvendes til validering, på en sådan måde, at der spærres for kort med numre, der dækker over forudbetalte kort. BIN-tabellerne opdateres med jævne mellemrum, og udbyderen vil i forbindelse med disse opdateringer skulle ajourføre sin software.

I modsætning til hovedparten af de øvrige former for elektronisk validering, er betalingskortmodellen forbundet med den betydelige fordel, at den kan anvendes af udlændinge (med udenlandske kort) på lige fod med danskere.

Omvendt kan modellen være forbundet med den ulempe, at brugerne efter omstændighederne ville kunne være tilbageholdende med at videregive oplysninger om betalingskort på internettet særligt i forbindelse med tjenester, som angiver at være gratis.

10.4. NemID-modellen

NemID er udviklet til at blive borgernes almindelige adgang til netbanker, offentlige selvbetjeningsløsninger samt en række private tjenester på nettet, der understøtter digital signatur.

Brugerens adgang med NemID til bl.a. de offentlige selvbetjeningsløsninger sker via en såkaldt to-faktor autentifikationsløsning, hvor adgangen er beskyttet af en personlig adgangskode og en kode fra et nøglekort med engangsnøgler. Brugerne skal i forbindelse med login angive et bruger-id, en personlig adgangskode og en engangskode fra det personlige nøglekort.

I den udstrækning den enkelte udbyder anvender NemID til brugeridentifikation, vil oplysninger om den enkelte brugers identitet blive opbevaret af DanID. DanID logger den relevante IP-adresse, andre oplysninger om den computer, der anvendes til login, samt det anvendte bruger-id. De pågældende oplysninger bliver opbevaret af DanID i minimum 5 år.

I Rudersdal Kommunes borgerservicecentre er der via stationære computere adgang til et begrænset antal internetsider. Adgangen hertil kræver ikke login eller lignende.

Der stilles endvidere trådløst internet til rådighed i de pågældende borgerservicecentre. Adgangen hertil sker via NemID og er ikke begrænset til særlige sider.

En åbenlys fordel ved NemID-modellen er, at den bygger på et gennemarbejdet nationalt projekt, som borgerne generelt vil kunne anvende til offentlige selvbetjeningsløsninger, netbanker mv.

I forhold til anvendelsen af NemID bemærkes det, at NemID som udgangspunkt forudsætter, at brugeren er fyldt 15 år. Endvidere er NemID-systemet knyttet op på bl.a. CPR-nummer og vil derfor – i lighed med CPR-modellen – kun i begrænset omfang kunne benyttes af udlændinge.

Herudover kan NemID på nuværende tidspunkt ikke anvendes på mobilteletelefoner med internetadgang. Det forventes imidlertid, at en sådan anvendelse vil være mulig inden for en kortere årrække.

10.5. Registrering på baggrund af forevist billedlegitimation

Endelig vil validering af en internetbrugers identitet kunne ske manuelt ved fremvisning af billedelegitimation. Det vil kunne ske ved, at der, på steder hvor internetadgang stilles til rådighed for brugere, og hvor der er personale til stede (f.eks. internetcaféer, biblioteker mv.), kræves fysisk fremvisning af billedlegitimation.

Behovet for en tilstrækkelig sikker validering af brugernes identitet vil ud fra en politifaglig vurdering forudsætte, at personalet de pågældende steder er særligt godkendt til at foretage denne form for validering, og at der foruden personidentitet også registreres oplysninger om den fremviste legitimation, eksempelvis et pas- eller kørekortnummer.

I en række sammenhænge, hvor udbyderen enten har et ønske om eller er forpligtet til at sikre, at alle kan få adgang til internettet, vil det antageligvis kunne være nødvendigt at supplere en elektronisk registreringsmetode med en sådan manuel model. Den manuelle model vil således (i den udstrækning man måtte ønske det) kunne lukke de huller, som er knyttet til de øvrige modeller i forhold til udlændinge og personer uden mobiltelefon eller betalingskort.

10.6. Vurderingen af modeller til validering af brugeridentiteten

De ovenfor skitserede modeller til validering af identiteten på internetbrugere vil i princippet alle kunne indrettes på en sådan måde, at de yder tilstrækkelig sikkerhed for brugerens identitet. Samtidig rummer de hver for sig en række fordele, men i visse tilfælde også nogle uhensigtsmæssigheder.

I lyset af den konstante teknologiske udvikling inden for internetkommunikation og identifikationsmidler samt den enkelte udbyders interesse i at kunne indrette sig efter lovgivningen på den for den pågældende mest hensigtsmæssige måde, finder arbejdsgruppen ikke anledning til at anbefale en bestemt model for registrering af brugeroplysninger frem for en anden.

Det bør således overlades til den enkelte part at vælge en effektiv løsning til sikring af en valideret registrering af brugernes identitetsoplysninger. I den udstrækning validiteten af de registrerede brugeroplysninger er lige så sikker, vil en løsning således også kunne baseres på andre modeller end de ovenfor skitserede.

Det bemærkes i den forbindelse, at det ikke vil kunne udelukkes, at vurderingen af en given løsning, som i dag måtte vurderes at leve op til de stillede krav, over tid vil kunne ændre sig.

Det afgørende vil i alle tilfælde være, at de registrerede oplysninger med tilstrækkelig sikkerhed kan føres tilbage til den faktiske bruger af internetadgangen, og at den pågældende i øvrigt ikke får adgang til internettet, før validering og registrering har fundet sted.

11. Arbejdsgruppens overvejelser om økonomiske og administrative konsekvenser

11.1. Konsekvenser af indførelse af en ordning om brugerregistrering for udbydere der i forvejen er omfattet af logningsforpligtelsen

I dag foretager udbydere i vidt omfang registrering og kontrol af identitetsoplysninger, der afgives af den enkelte kunde i forbindelse med indgåelse af en internet-abonnementsaftale.

Denne kontrol gennemføres i praksis enten i forbindelse med kundens anvendelse af et betalingskort eller ved, at den pågældende – udover oplysninger om navn og adresse mv. – oplyser sit personnummer, hvorefter teleudbyderen via Det Centrale Personregister sammenholder personnummeret med de øvrige kundeoplysninger.

Indførelsen af et krav om registrering af validerede brugeroplysninger vil således i praksis ikke få betydning for den registrering af brugeroplysninger, der i dag foretages i forbindelse med abonnementsaftaler og lignende.

På baggrund af de oplysninger, som arbejdsgruppen har indhentet hos leverandører af internetadgang, er det arbejdsgruppens vurdering, at indførelse af en pligt til at registrere og validere brugeroplysninger alene vil være forbundet med forholdsvis begrænsede merudgifter for de udbydere, der allerede i dag er omfattet af logningsforpligtelsen, men

som ikke i dag registrerer og validerer brugeroplysninger (jf. nærmere eksemplerne i afsnit 11.2 nedenfor).

Denne vurdering understøttes af, at en række udbydere mv. allerede i dag anvender softwareløsninger, der bl.a. har til formål at tilvejebringe oplysninger om den faktiske brugers identitet, uanset de pågældende udbydere hverken har et forretningsmæssigt behov herfor eller er forpligtede hertil (jf. eksempelvis nedenfor om logningspakker til lystbådehavne mv., der er baseret på brugerens angivelse af en e-mail-adresse, og det ovenfor anførte om Odense Universitetshospitals anvendelse af en model, hvor valideringen sker ud fra et af brugeren angivet CPR-nummer).

11.2. Konsekvenser af en udvidelse af kredsen af pligtsubjekter efter logningsbekendtgørelsen til også at omfatte en række ikke-kommercielle aktører

Udvidelse af kredsen af pligtsubjekter efter logningsbekendtgørelsen til også at omfatte parter, der på ikke-kommercielt grundlag stiller internetadgang til rådighed for en ikke på forhånd afgrænset kreds af slutbrugere, må særligt forudses at få betydning for biblioteker og kommunale servicecentre mv. Endvidere vil det være nødvendigt for en række aktører, herunder uddannelsesinstitutioner, hospitaler og større arbejdspladser, som ikke ønsker at blive omfattet af logningsforpligtelsen, at tage skridt med henblik på at sikre, at deres brugerkreds er tilstrækkeligt afgrænset.

Sealink Technology ApS, som bl.a. leverer trådløse internetløsninger til en række havne og hoteller samt Det Kongelige Teater, har over for arbejdsgruppen oplyst, at man på nuværende tidspunkt leverer logningspakker til hoteller til priser fra 1.495 kr. pr. måned. For lystbådehavne er prisen fra 795 kr. pr. måned, mens små hotspots (med et access point) betaler fra 495 kr. pr. måned. Til de nævnte logningspakker, der er angivet i priser eksklusive moms, er knyttet et oprettelsesgebyr på 2.995 kr.

Logningspakkerne inkluderer bl.a. software til brugeridentifikation baseret på en e-mail-model, hvor en adgangskode sendes til en e-mail-adresse, der er angivet af brugeren, og en betalingskort-model, hvor oplysninger om kundens identitet registreres i form af et betalingskortnummer, som kunden oplyser i forbindelse med, at der med et beta-

lingskort betales for adgangen til internettet (jf. også afsnit 9.3. ovenfor).

Sealink Technology ApS har oplyst, at såfremt man ønsker at anvende en betalingskort-model, hvor der gennemføres en forespørgsel vedrørende et betalingskorts gyldighed mv., uden at der i den forbindelse trækkes et beløb fra kortet (såkaldt preauth), vil de ovenstående priser i stedet være fra 2.190 kr. (hoteller), fra 1.190 kr. (lystbådehavne) og fra 690 kr. (små hotspots). Hertil skal lægges et oprettelsesgebyr på 7.990 kr. (hoteller), 5.490 kr. (lystbådehavne) og 4.490 kr. (små hotspots) samt eventuelle gebyrer, som opkræves af Nets (eller anden international virksomhed, der håndterer betalinger med internationale betalingskort) for undersøgelsen vedrørende det pågældende kortnummers gyldighed og eventuel spærring af spærret.

Det er Sealink Technology ApS' vurdering, at de fleste kommunale biblioteker kan sammenlignes med små hotspots (med et access point), og at den økonomiske byrde for et bibliotek, der omfattes af logningsforpligtelsen, vil svare til omkostningerne ved driften af et lille hotspot.

Buttler Networks, der bl.a. har varetaget logning på vegne af Commute Media (tidligere Gratis Danmark) i S-tog og på en række buslinjer, har over for arbejdsgruppen oplyst, at man formentlig vil kunne købe software med en login-funktion for ca. 2.000 kr. ved op til 20 brugere eller for ca. 5.000 kr. ved et ubegrænset antal brugere. Vurderingen er dog foretaget uden nærmere kendskab til, i hvilket omfang den givne software vil opfylde de krav til brugeridentifikation, der er nærmere beskrevet ovenfor. Buttler Networks har endvidere oplyst, at en egenudvikling af software med en login-funktion vil koste omkring ca. 200.000 kr.

Buttler Networks vurderer, at sådanne merudgifter til indkøb eller egenudvikling af software med en login-funktion vil resultere i en forholdsvis beskeden forhøjelse af det beløb, udbyderne i dag betaler for at få foretaget logning.

11.3. Konsekvenser af at ophæve logningsforpligtelsen for en række kommercielle udbydere

Ved at ændre kredsen af logningsforpligtede som ovenfor anført, vil en række kommercielle udbydere af internettjenester, som i dag vil skulle

foretage logning i overensstemmelse med bekendtgørelsens regler, blive frigjort for denne forpligtelse.

Om de økonomiske besparelser herved kan der henvises til det, der er anført umiddelbart ovenfor under pkt. 11.2.

Det har i den forbindelse endvidere været væsentligt for arbejdsgruppen at sikre, at man i videst muligt omfang undgår at pålægge udbydere udgifter (selv om de samlet set er begrænsede) og forpligtelser, som ikke er politimæssigt velbegrundede.

Det har i forlængelse heraf været arbejdsgruppens opfattelse, at det af konkurrencemæssige grunde er rigtigst ikke at pålægge eksempelvis privathospitaler og private uddannelsesinstitutioner byrder, som ikke påhviler tilsvarende offentlige institutioner, medmindre der er helt særlige grunde, der taler herfor.

12. Arbejdsgruppens overvejelser om "huller" i den skitserede model

Det har været arbejdsgruppens opfattelse, at indførelse af yderligere krav om brugerregistrering og logning alene bør indføres i den udstrækning, der vil være tale om en reel og væsentlig forbedring af politiets og anklagemyndighedens mulighed for at efterforske og retsforfølge terrorisme og anden alvorlig kriminalitet.

Arbejdsgruppen har således tilstræbt at skitsere en model for brugerregistrering, som i betydelig grad vanskeliggør muligheden for, at kriminelle grupperinger mv. ubesværet og inden for lovgivningens rammer kan vælge at kommunikere over internettet på en måde, som sikrer, at trafikken ikke logges, og at de kommunikerende parters identitet ikke kan klarlægges.

Det har således været arbejdsgruppens hensigt at skitsere en løsningsmodel, der i praksis vil sikre, at politiet og anklagemyndigheden – når betingelserne for at foretage indgreb i meddelelseshemmeligheden er til stede – ved sådanne indgreb eventuelt suppleret med andre traditionelle efterforskningsmetoder vil kunne afdække identiteten på personer, der har kommunikeret over internettet.

Arbejdsgruppen er imidlertid opmærksom på, at det selv med en relativt vandtæt model for brugerregistrering i nogen grad vil være muligt at

omgå reglerne, ligesom andres uforsigtige anvendelse af eksempelvis trådløse net også vil kunne åbne mulighed for, at kriminelle grupperinger kan kommunikere på måder, som vanskeliggør politiets og anklagemyndighedens efterforskning af alvorlig kriminalitet.

12.1. Private usikrede net

Arbejdsgruppen har i den forbindelse særligt drøftet de problemer, der vil kunne være forbundet med, at ikke alle private borgere har sikret deres private trådløse net.

I den udstrækning et net ikke er blevet sikret, fordi indehaveren af nettet ønsker, at andre i almindelighed skal kunne benytte nettet, vil den pågældende efter den skitserede model blive omfattet af logningsforpligtelsen og i den forbindelse også af brugerregistreringsordningen. I den forbindelse bemærkes i øvrigt, at såfremt et privat trådløst net bevidst stilles til rådighed for andre end personer i husstanden, vil det efter omstændighederne kunne udgøre et brud på leveringsaftalen med udbyderen.

Hvor den manglende sikkerhed omkring nettet alene skyldes uforsigtighed eller manglende teknisk indsigt, og indehaveren af nettet ikke har ønsket at lade andre benytte nettet, er det arbejdsgruppens opfattelse, at den pågældende ikke vil blive omfattet af logningsforpligtelsen.

Det er imidlertid i den forbindelse arbejdsgruppens vurdering, at private borgere i stigende grad er opmærksomme på betydningen af at sikre deres net, og at antallet af usikrede private net derfor er faldende.

Det er samtidig arbejdsgruppens vurdering, at antallet af usikrede net fortsat er betydeligt, hvilket bl.a. må antages at hænge sammen med, at en betydelig del af de trådløse internetløsninger, der sælges i dag, typisk leveres og opsættes i usikret tilstand (eller sikret med en standardkode, som meget let kan findes ved en søgning på internettet), således at indehaveren selv skal aktivere en sikkerhedsforanstaltning, hvis nettet skal sikres.

Arbejdsgruppen har i den forbindelse overvejet, om man burde stille krav om, at trådløse internetløsninger, når de leveres eller installeres, skal være sikret med en brugerkode, så det vil kræve en aktiv handling at åbne nettet for udenforstående.

Det er imidlertid været arbejdsgruppens umiddelbare vurdering, at det af hensyn til brugervenligheden og smidigheden i forbindelse med opsætning og installation er en betydelig fordel for brugeren, at nettet kan "startes" i en ubeskyttet tilstand.

Øget oplysning kan formentlig medvirke til at begrænse forekomsten af usikrede net, idet indehaverne af de private trådløse net generelt vil have en egen interesse i at sikre deres net.

Denne interesse vil dels bestå i at forebygge, at brugerens egen trafik bliver hæmmet i kraft af, at andre belaster forbindelsen, dels i at forebygge, at man kommer i politiets søgelys i forbindelse med, at andre har anvendt ens net til at kommunikere i forbindelse med kriminelle aktiviteter.

I tilknytning hertil bemærkes i øvrigt, at naboer, forbipasserende mv., der uberettiget via en ikke-sikret trådløs internetforbindelse, som tilhører en anden, foretager opkobling på internettet og efterfølgende anvender denne internetforbindelse, som udgangspunkt vil overtræde straffelovens § 293, stk. 1, om brugstyveri.

12.2. Misbrug af andres identitet

Arbejdsgruppen har drøftet de mulige udfordringer, der knytter sig til risikoen for, at andres identitetsoplysninger misbruges i forbindelse med, at personer skaffer sig adgang til internettet.

Et sådant misbrug vil normalt udgøre et selvstændigt strafbart forhold. Det er således arbejdsgruppens opfattelse, at eventuelle udfordringer i denne retning må behandles som andre overtrædelser af de regler, der gælder på området, og således ikke udgør et særligt problem i forhold til den her skitserede model.

Hvis der i forbindelse med en elektronisk valideringsproces afgives identitetsoplysninger, som vedrører en anden, end den person, der søger at opnå adgang til internettet, vil det som udgangspunkt udgøre en overtrædelse af straffelovens § 171 om dokumentfalsk.

Fremvises der i forbindelse med en "manuel" identifikationsproces et legitimationsdokument, der ikke knytter sig til den person, der fremvi-

ser dokumentet, og således ikke vedrører den person, der søger at få adgang til internettet, vil det som udgangspunkt udgøre en overtrædelse af straffelovens § 174 om dokumentmisbrug.

Endvidere må det antages, at et misbrug af identitetsoplysninger eller legitimationspapirer ofte vil være baseret på et forudgående tyveri af et identitetsdokument (kørekort, sygesikring, pas eller lignende).

Politiet har i forbindelse med arbejdsgruppens arbejde tilkendegivet, at det også i denne situation vil udgøre et betydeligt løft i politiets mulighed for at efterforske på baggrund af internetkommunikation, hvis politiet har oplysninger om identiteten på en person, som enten havde kendskab til, hvem der måtte have anvendt den pågældendes identitet, eller som har været udsat for et tyveri eller lignende, som vil kunne danne grundlag for en strafferetlig efterforskning.

Samtidig vil det forbedre mulighederne for relativt hurtigt at skride ind over for et misbrug af en given identitet. Sker misbruget således med samtykke fra den, som oplysningerne rettelig vedrører, vil dette efter omstændighederne kunne sanktioneres som medvirken. Sker det uden et sådant samtykke, vil det i hvert fald i forhold til elektronisk identifikation på baggrund af NemID, betalingskort eller mobiltelefon være muligt at spærre det pågældende identifikationsmiddel, hvorved fremtidig identifikation på grundlag heraf vil være afskåret. Det bemærkes i tilknytning hertil, at validering baseret på CPR-modellen vil kunne udgøre et særligt problem i denne sammenhæng, idet det som nævnt ovenfor vil kunne være vanskeligt at skride effektivt ind over for misbruget, hvis det konstateres, at et CPR-nummer og tilhørende identitetsoplysninger anvendes af en anden, end den det tilhører.

12.3. Anvendelse af udenlandske mobile bredbånd og taletidskort på det danske net

12.3.1. Arbejdsgruppen har endvidere drøftet, hvilke udfordringer der ligger i, at aftaler om levering af mobilt bredbånd, uanset om de har form af egentlige abonnementer eller af en given mængde forudbetalt internettrafik, vil kunne tænkes erhvervet i udlandet og anvendt på det danske net. Arbejdsgruppen har i tilknytning hertil drøftet den tilsvarende problemstilling for så vidt angår mobiltelefonabonnementer og taletidskort, når adgang til internettet opnås via en mobiltelefon.

12.3.2. For så vidt angår egentlige abonnementsaftaler på mobilt bredbånd, vil de problemer, der vil kunne være forbundet med at fastlægge identiteten på brugerne heraf, svare til de udfordringer, der gør sig gældende for almindelig telefoni. Der vil således normalt være muligt for politiet at indhente brugeroplysninger fra det land, hvor abonnementet er hjemmehørende.

På baggrund af oplysninger fra de centrale udbydere af mobilt bredbånd er det arbejdsgruppens vurdering, at det formentlig i dag er meget begrænset, i hvilken udstrækning mobilt forudbetalt bredbånd, der erhverves i udlandet, kan anvendes i Danmark.

De priser, der normalt vil være forbundet med at kommunikere over internettet på grundlag af et forudbetalt mobilt bredbånd i udlandet, er i dag typisk så høje, at det hidtil ikke har været attraktivt for udbyderne at åbne for trafik på et udenlandsk net.

Det er imidlertid arbejdsgruppens vurdering, at det over tid meget vel vil kunne blive attraktivt for udbyderne at åbne for trafik på udenlandske net, f.eks. hvor den pågældende udbyder har mulighed for at benytte egne net i flere lande eller som en konsekvens af faldende roamingpriser.

Herudover kan det ikke udelukkes, at indførelsen af en registreringsordning i sig selv vil kunne medvirke til, at kriminelle i stigende grad vælger at benytte sig af et forudbetalt – "anonymt" – mobilt bredbånd.

Man må således forudse, at udenlandske forudbetalte mobile bredbånd på et tidspunkt vil kunne komme til at spille en rolle også på det danske net.

Det er i den forbindelse arbejdsgruppens vurdering, at det vil være teknisk vanskeligt – om overhovedet muligt – at konstatere, om et udenlandsk mobilt bredbånd, som anvendes på det danske net, er forudbetalt eller baseret på en abonnementsaftale.

Det er samtidig arbejdsgruppens vurdering, at selv om det vil være teknisk muligt generelt at identificere udenlandske mobile bredbånd, vil en ordning, hvorefter brugere af alle sådanne bredbåndsløsninger enten afskæres adgangen til det danske net eller vil skulle identificere sig hver gang de går på et dansk net, i praksis komme til at indebære en ikke

ubetydelig restriktion i forhold til den grænseoverskridende anvendelse af disse tjenester.

Det er på den baggrund arbejdsgruppens opfattelse, at der ikke på nuværende tidspunkt er tilstrækkeligt grundlag for at indføre særlige krav med henblik på at dæmme op for anvendelsen af forudbetalte udenlandske mobile bredbånd på det danske net. Der vil imidlertid være behov for at følge udviklingen på dette område nøje.

12.3.3. Mens det i dag som nævnt vurderes, at der kun i meget begrænset omfang kan kommunikeres med udenlandsk erhvervede forudbetalte mobile bredbåndsløsninger i Danmark, forholder det sig anderledes med udenlandske taletidskort.

Det vil således være muligt for personer, som går på internettet ved brug af deres mobiltelefon at gøre dette på grundlag af et udenlandsk uregistreret taletidskort.

På baggrund af oplysninger fra udbydere af uregistrerede taletidskort er det i imidlertid arbejdsgruppens vurdering, at det prisniveau, der i dag er gældende for internettrafik baseret på udenlandske taletidskort ligger så højt, at det ikke er sandsynligt, at denne kommunikationsform vil blive udbredt som grundlag for internetkommunikation, heller ikke i kredse som generelt gerne ønsker at unddrage sig myndighedernes søgelys. Omvendt er det givet, at det vil være en kommunikationsform, der af kriminelle netværk vil kunne vælges i forbindelse med enkeltstående kommunikation, som der er et særligt konkret ønske om at sikre, ikke kan henføres til den pågældende bruger.

Det er imidlertid arbejdsgruppens umiddelbare vurdering, at kommunikation i disse særlige situationer fortrinsvis vil være baseret på almindelig mobiltelefoni snarere end internetbaseret kommunikation, hvorfor problemstillingen ikke i praksis øger de udfordringer, som er forbundet med udenlandske uregistrerede taletidskort, der anvendes til mobiltelefoni.

13. Opsamling og anbefalinger

I medfør af de gældende regler i logningsdirektivet og logningsbekendtgørelsen registreres og opbevares der i dag en ganske omfattende mængde oplysninger om internettrafik.

På trods heraf er der inden for rammerne af de gældende regler ganske vid adgang til, at de, der ønsker at kommunikere på en måde, som i praksis kun meget vanskeligt vil kunne afdækkes i forbindelse med eksempelvis en strafferetlig efterforskning, kan gøre dette.

Enhver kan således i dag fuldt lovligt vælge at benytte en kommunikationsform, som sikrer, at den pågældendes identitet ikke kan afdækkes, og som foregår under omstændigheder, hvor oplysninger om internettrafikken ikke registreres, og således ikke kan tilvejebringes, selv om retsplejelovens betingelser for indgreb i meddelelseshemmeligheden er opfyldt.

Denne vide adgang til at "omgå" reglerne i logningsbekendtgørelsen udgør efter arbejdsgruppens opfattelse ikke kun et problem i forhold til politiets og anklagemyndighedens opklaring af alvorlige forbrydelser (jf. afsnit 6 og 7 ovenfor), men rejser også spørgsmål i forhold til rimeligheden af (kun) at pålægge de kommercielle udbydere en logningsforpligtelse og i forhold til det principielt rigtige i at sikre tilstedeværelsen af betydelige mængder oplysninger om "lovlydige borgeres" kommunikation, når det samtidig må antages, at en betydelig del af den kommunikation, som udveksles i et ulovligt øjemed, må forventes ikke at blive registreret eller i hvert fald ikke vil kunne henføres til konkrete personer.

Det er arbejdsgruppens samlede vurdering, at det vil være teknisk muligt at indføre en ordning med registrering af brugere af internetforbindelser, som vil kunne udgøre et betydeligt løft i politiets mulighed for at efterforske på baggrund af internetkommunikation i forhold til de muligheder, som politiet har i dag, og uden at det vil indebære en reel begrænsning i den almindelige adgang til internettet for borgere og virksomheder i Danmark.

Det er i forlængelse heraf arbejdsgruppens vurdering, at en eventuel brugerregistreringsordning i givet fald bør ledsages af en ændring af kredsen af pligtsubjekter efter logningsbekendtgørelsen, således at kredsen af pligtsubjekter ikke afgrænses på baggrund af et kommercialitetskriterium, men på baggrund af, om den pågældende aktør stiller internetadgang til rådighed for en "ikke på forhånd afgrænset kreds" af brugere. På den måde vil der i forhold til logningsforpligtelsen blive

skabt parallelitet mellem henholdsvis kommercielle og ikke-kommercielle udbydere.

Det er således arbejdsgruppens opfattelse, at en ændring af kredsen af logningsforpligtede kombineret med en brugerregistreringsordning ikke alene vil forbedre politiets og anklagemyndighedens efterforskningsmuligheder, men også – bl.a. i kraft heraf – vil kunne mindske de betænkeligheder af såvel principiel som ressourcemæssig art, der har været fremført i forhold til proportionaliteten i den nugældende ordning.

Arbejdsgruppen har peget på en række modeller til sikring af en valideret brugerregistrering, som vil være praktisk anvendelige. Arbejdsgruppen har imidlertid ikke fundet anledning til at anbefale én bestemt model for registrering af brugeroplysninger, som alle leverandører af internetforbindelser i givet fald vil skulle anvende.

I lyset af den konstante teknologiske udvikling inden for internetkommunikation og identifikationsmidler samt den enkelte udbyders interesse i at kunne indrette sig efter lovgivningen på den for den pågældende mest hensigtsmæssige måde, finder arbejdsgruppen således, at det i givet fald bør overlades til den enkelte leverandør at vælge en effektiv model til sikring af en valideret registrering af brugernes identitetsoplysninger.

Det vil imidlertid være en afgørende forudsætning for anvendelsen af en given registrerings- og valideringsmodel, at brugeren ikke får adgang til internettet, før oplysningerne om den pågældendes identitet er registreret hos udbyderen, og at identifikationen er entydig og bygger på oplysninger, der umiddelbart kan valideres med henblik på at sikre rigtigheden heraf.

I forhold til byrderne for de parter, der i givet fald vil blive omfattet af en pligt til at registrere og validere brugeroplysninger mv., er det endvidere arbejdsgruppens opfattelse, at indførelse af en sådan ordning vil være forbundet med visse omkostninger, særligt for de leverandører af internetforbindelser, som ikke i dag er omfattet af logningsforpligtelsen (det vil først og fremmest sige offentlige myndigheder og institutioner). På baggrund af de oplysninger, som arbejdsgruppen har indhentet fra en række leverandører af logningsløsninger, vurderes det dog, at omkostningerne ikke kan siges at stå i misforhold til den samfundsmæssige

gevinst i forhold til opklaring og forebyggelse af alvorlig kriminalitet, der vil være forbundet med en sådan ordning.

For så vidt angår kommercielle udbydere (der i dag er omfattet af logningsforpligtelsen), men som alene stiller internet til rådighed for en på forhånd afgrænset kreds af brugere, vil den skitserede model medføre en økonomisk og administrativ lettelse, idet disse udbydere ikke længere vil skulle foretage logning i medfør af bekendtgørelsen.